

WMS Pro Help Manual

This manual applies to WMS Pro 3.3

New editions of this manual will be updated when the version release updates.

Table of Contents

Introduction	3
Dashboard	4
Alarms.....	4
Site maps.....	10
Cardholders.....	13
Region occupancy	19
Credentials	20
Controller Access Groups	22
Timezones	29
Holidays.....	31
Unified Access Groups	33
History logs	35
Reports.....	36
Status & control	38
Controllers.....	40
Devices	44
Automations.....	47
External API's	49
Maps	51
Regions.....	54
Sites	56
Holiday types	58
Card programmers	59
Reader Configuration cards.....	61
Departments	64
Custom fields	66
Credential groups	68
Card maintenance	70
Alarm responses	71
Roles	72
Operators	74
Settings	77
About	80

Introduction

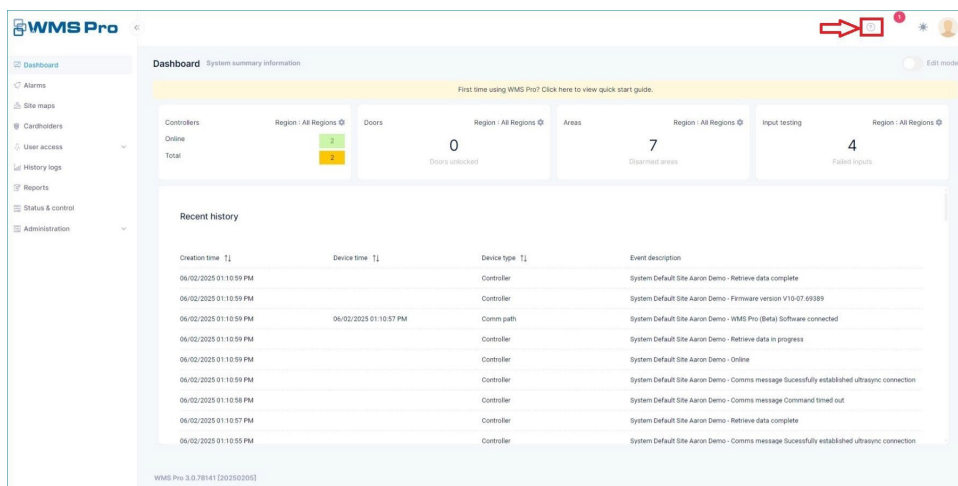
WMS Pro Installation Guide and Quick Start Guides are available at the following web links:

<https://support.firesecurityproducts.com.au/hc/en-us/articles/7108394505743-WMS-Pro-Quick-Start-Guide>

<https://support.firesecurityproducts.com.au/hc/en-us/articles/7108329287567-WMS-Pro-Installation-Guide-and-Datasheet>

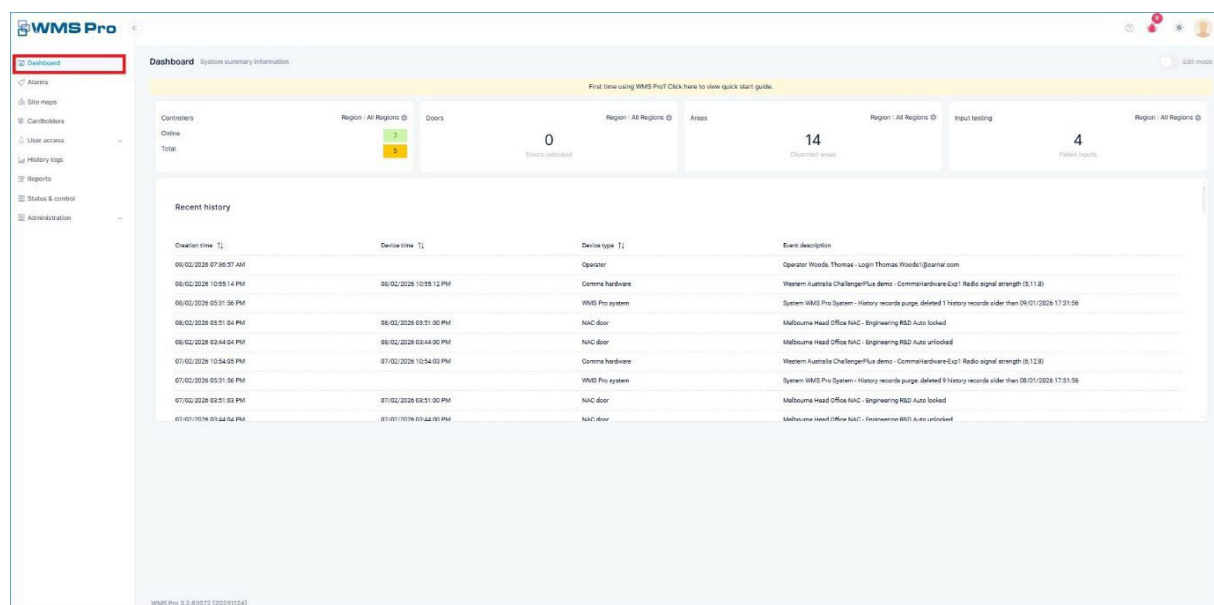


All information contained in this WMS Pro Help Manual is from the latest version of WMS Pro and can be found by clicking on the '?' in the top right hand side of every page in this site. See below.



Dashboard

System summary information



Basic page functionality

WMS Pro logo

Clicking on the application logo found in the top-left will direct you to the Dashboard. The application logo can be customised in the [Settings](#) page.

Navigation sidebar

The sidebar on the left will contain all the menu option pages in WMS Pro. Click the << button to collapse or expand the sidebar.

? Help menu

Help content is directly integrated on every page of WMS Pro. Click the icon expand the help panel, which will display helpful information for the current page.

Alarms

Redirects the current page to the [Alarms](#) page. This option is only available if the appropriate [license](#) has been applied to WMS Pro.

Light Mode / Dark Mode

Click on the symbol to toggle between light mode and dark mode. By default WMS Pro will be in light mode, changing to dark mode will change the overall colour theme to a darker colour and is a purely **cosmetic** change.

Profile settings

Clicking on the profile image on the top right of the page will bring up a drop-down menu containing several options:

- ...
-  • Change password
-  • Change profile picture
-  • My settings
 - First name and Surname
 - Email address
 - Login name
 - Enable Authenticator App - When you click on the 'Enable Authenticator App' you will be brought to a 3 step 'Two Factor Authentication' where you will need to:

1. WMS Pro generates a QR code, which should be scanned by the Operator's 2FA/MFA app.
2. Once scanned and added to their app, the Operator will need to enter the current 6 digit code being displayed.
3. WMS Pro will validate the code, and if everything matches it will complete the set-up and display a list of Recovery codes that can be used as backup (e.g. if the account and/or app is unavailable, lost, stolen, etc.) **Note:** To change Recovery codes, you must disable then re-enable app-based 2FA.

-  My preferences
 - Hide quick start guide checkbox - removes the quick start guide banner found in the dashboard
 - Alarm sound preference - set the alarm sound that will play when an Alarm is triggered; press the  button to test the Alarm
 - Alarm snooze timeout (Minutes)* - set the alarm snooze timeout in minutes. Use the up and down arrow to adjust the number of minutes. Default is set to 10 minutes.
 - Default map - select your default map to be displayed when you navigate to the [Site maps](#) page.
-  Logout

WMS Pro System Warning Banner Summary

The WMS Pro application displays critical system warnings in a header banner to alert administrators of issues requiring immediate attention. The logic behind it is as follows:

- Warnings follow strict priority hierarchy
- Higher priority warnings suppress lower priority ones
- Real-time monitoring through license service subscription
- Automatic updates when system conditions change

This warning system ensures administrators are immediately notified of the most critical system issues first, preventing information overload while maintaining system reliability awareness.

The following Warning types and priority are displayed as follows:

- **License Warning** (Critical - Highest Priority) - Triggered by Invalid or expired license. Links to license administration page if user has permissions. Blocks other warnings from displaying.
- **Service Warning** (High Priority) - Triggered by Communication or event service not running. Only displays if license is valid.
- **Disk Space Warning** (Medium Priority) - Triggered by Disk space usage $\geq$ 80%, 90% or 95%. Only displays if license is valid and services are running.

System summary information

The banner at the top of the dashboard page contains a link to the [WMS Pro quick start guide](#). To hide the banner, change the settings under the  **My preferences** profile settings (See the **Basic page functionality** section at the top of this article).

The dashboard page contains a collection of widgets that provide a quick view of the overall system status.

The current status information by default is set to **All Regions**, this can be configured by clicking on the  symbol. A pop-up window will then appear and give the [Operator](#) the option to choose their desired [Region](#). Choosing a specific Region will filter the status information to only display the results for said Region.

Widgets

Widgets provide a quick and easy means of viewing and interacting with your system. Widgets are designed to facilitate simple interactions, such as tapping on some information or clicking a button, which then responds by performing a command, such as navigating to a relevant page.

A list of WMS Pro widgets and their interactions can be found below:

Controllers

Displays the number of [Controllers](#) currently online, and the total number currently enrolled in WMS Pro. Please note that this number reflects both Controllers and NACs.

Interacting with the online/total section will direct Operators to the [Controllers](#) page.

Doors

Displays the number of Doors currently unlocked.

Interacting with the number unlocked section will direct Operators to the [Status & Control](#) page, with a filter automatically applied to show a list of Doors with an Unlocked status.

Areas

Displays the number of Areas currently disarmed (accessed).

Interacting with the number disarmed section will direct Operators to the [Status & control](#) page, with a filter automatically applied to show a list of Areas with an Accessed status.

Input testing

Provides the number of Inputs which have failed to test.

Interacting with the failed input section will direct Operators to the [Status & control](#) page, with a filter automatically applied to show a list of Inputs.

- **Additional info:**
 - Input testing must be configured on the hardware separately to ensure the widget provides accurate information. Input testing is performed when a configured input is activated during an access/secure test or normal operation, depending on the required type of activation. Each input requiring input testing must be programmed with both a test type and test days, and will report a test failed event when it has not been activated within the specified number of days.
 - When viewing the filtered Status & control page, WMS Pro will display a list of all inputs on the system. If a list of inputs with a test fail event is required, Operators may use a [History report](#) with the 'Event filter' set to 'Test fail', and the 'Second event filter' set to 'Test fail restored'. This will generate a report that may be used to view Inputs which have generated test fail events, and may be easily filtered further using the Excel format. These parameters may also be saved as a Report template for integration with [Automations](#) and/or quick access for future use.

Recent History

The Recent history list displays events that have occurred on WMS Pro and enrolled devices, such as Operator activity, Cardholders arming areas, doors being accessed, etc. This event list is automatically refreshed, with new events typically appearing within a few seconds of the event occurring.

Device in fault

This will show a window with the name Faults. It will give you a number of Devices in Fault.

Interacting with the number Faults section will direct Operators to the [Status & control](#) page, with a filter automatically applied to show the Device status information.

Custom button widget

This will show a window with the name Button. Use the Configure button to configure the Button text, Button colour and choose a Button event from the drop down. Save this screen to have it populated in the window on the Dashboard.

To create an [Automation](#) using a custom button widget, first create a Trigger from the Automations page. This trigger should be activated when the button on the widget is pressed. You can configure the Automation to perform an Action - for example, arming an Area.

Note: Multiple copies of the same widget with different settings can be added.

Edit mode

The Dashboard can be customised to display only the information the Operator wants to see. At the top right of the page is a slider for Edit mode, clicking on it will display a  on the top right of each widget and allow the Operator to remove them from the dashboard.

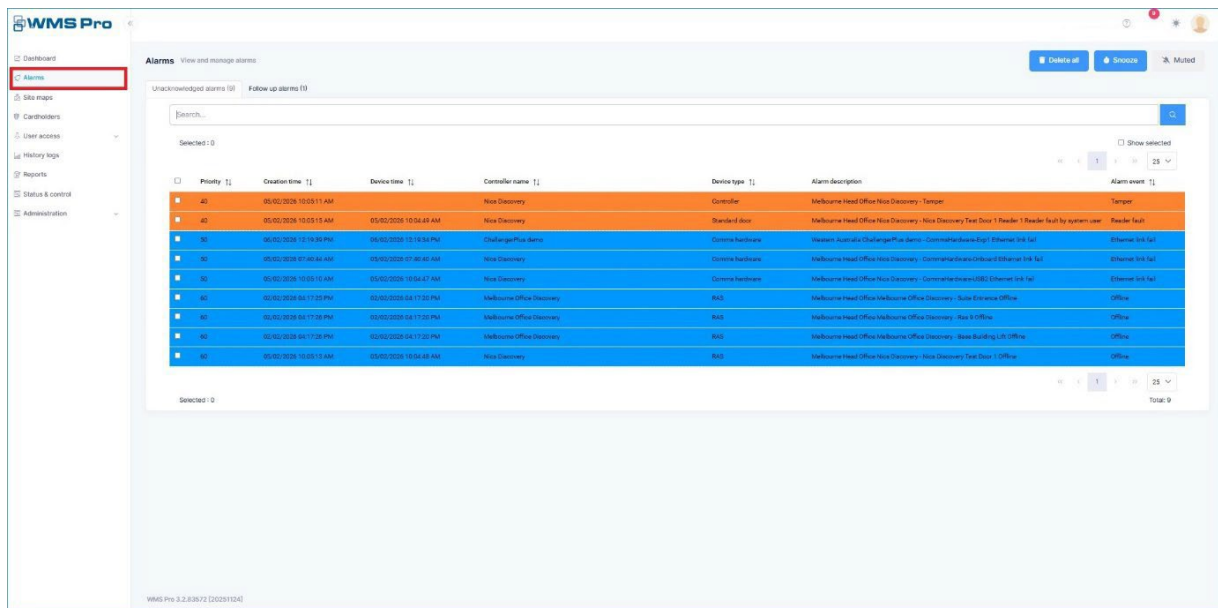
Widgets can be moved around in the dashboard by clicking and dragging the box around the page. They can also be resized by hovering the mouse over the edge of the widget and clicking and dragging.

At the bottom of the page is a toolbox that will allow the Operator to:

-  • Add widget
-  • Add page - creates a new tab that can be populated with widgets
-  • Rename page - renames said tab
-  • Convert page back to default - this option will be changed to "**Delete page**" if there are multiple pages
-  • Save any changes made

Alarms

View and manage alarms



Search bar

Enter a search term to narrow down the Alarm list to assist with locating a specific Alarm.



Delete all

Click the "Delete all" button to delete all of the Alarms.



Snooze

Click the Snooze button to temporarily "snooze" the Alarm for 10 minutes (Default) or until a new Alarm appears. Snooze timer can be adjusted by going into 'My preferences'.



Mute

Click the Mute button to silence the Alarm indefinitely until the Mute button is pressed again.

Unacknowledged alarms

Any unacknowledged Alarms reported by the **Controller** will appear in the list. The Alarms will be organised based on **priority**, Alarms with a lower number in the priority column will have a higher priority and appear further up the list.

Alarms can be deleted by hovering over the Alarm row and clicking on the  symbol. They can also be deleted in bulk by ticking the checkbox next to each Alarm you want to delete, then clicking on the  symbol in the bottom right.

Alarm details

Clicking on the Alarm event will open up a new pop-up window. This window will display the Alarm event history for the specific device.

It will also allow you to see the Device status and allow you to give it a quick action for the device via a drop down selection.

For example: If you have a device in alarm, you could 'Isolate' or 'Deisolate' the device (Command depends on device type) and click 'Execute' for a quick action.

Enter text in the "Enter response message" to provide a text description of the response provided to the Alarm. Once done click on the **Acknowledge** button.

Alternatively, click on the drop down bar to select from any of the [Alarm responses](#) that are available. Doing so will also populate the "Enter response message" field with text attached to the chosen Alarm response.

Multiple Alarms can be bulk acknowledged by ticking the checkboxes next to the Alarm name and pressing the  icon below the list.

Follow up alarms

When a still active Alarm is acknowledged in the unacknowledged tab, instead of disappearing they are moved to the "Follow up alarms" tab for follow up options. Once the Alarm is no longer active, it will be removed from this list.

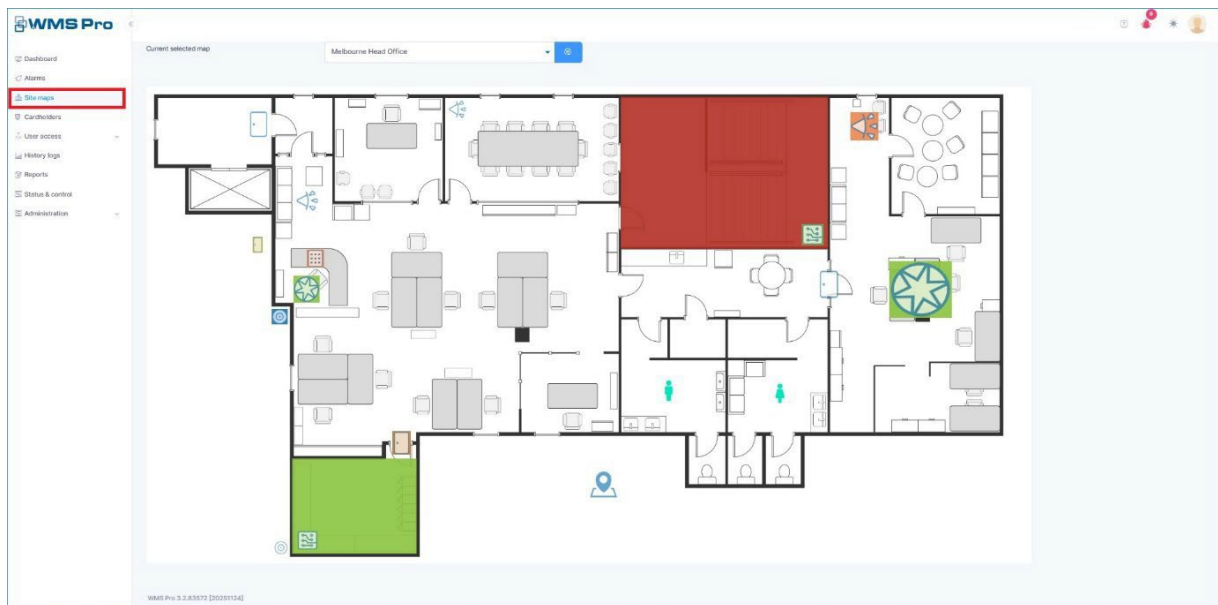
Alarm details

Same as above.

Alarm override screen

When an event arrives which is configured with both 'Alarm event' and 'Priority Alarm Overlay' enabled, and the logged in Operator(s) do not have 'Disable override alarm' permission enabled, a screen will appear over the top of the entire WMS Pro interface to block all input until the Operator clicks a button.

Site maps



Site maps are typically used to provide a graphical layout of the Site to Operators, with a focus on displaying the location and status of various devices, such as Areas, Inputs, Doors, Readers, etc. Maps must already be set up on the [Administration > Maps](#) page and belong to a [Region](#) which the [Operator](#) has permissions to view before they will appear on this page.

The default map that will be displayed when navigating to this page is configured by each Operator. To modify, Operators may click on their user icon at the top right of the page and select **My preferences**. Operators can change the map currently being displayed by selecting another one from the **Current selected map** list, either using the drop-down menu or by clicking on the advanced select icon to search and/or sort the list of maps available to the Operator.

When a map is displayed, it will automatically scale and adjust to fit within the available bounds of the web browser. If the available space in the web browser is altered (for example, by resizing a browser window, or rotating the display device), WMS Pro will make every effort to automatically adjust the map & device sizes and locations. In certain conditions, WMS Pro may have some difficulties correctly adjusting some elements, however this can typically be resolved by simply reloading the page, or navigating away and back again.

Devices and links to other maps are displayed as either an icon or a transparent area overlaid on a section of the background image. Each map item representing a device may also display a coloured background to indicate its current status, and/or a coloured border to represent an active alarm condition.

Device status colours

A description of each device's status colour codes can be found below:

Area

Accessed (disarmed)	Secured (armed)	Area stay (partial arm)	
------------------------	--------------------	----------------------------	--

Automation zone

On (On / Trigger / Level)	Off
------------------------------	-----

Controller

Online	Alarm / Tamper / Offline	Isolated	
--------	--------------------------	----------	--

DGP

Online	Alarm / Tamper / Offline	Isolated	
--------	--------------------------	----------	--

Door

Unlocked	Locked	Isolated	Disabled
----------	--------	----------	----------

Floor

Accessed / Auto accessed	Secured / Auto secure	
--------------------------	-----------------------	--

Input

	Alarm / Tamper	Isolated	
--	----------------	----------	--

Lift

	Disabled
--	----------

RAS

Online	Alarm / Tamper / Offline	Isolated	
--------	--------------------------	----------	--

Reader

	Disabled
--	----------

Relay

	Active	
--	--------	--

Additionally, devices in alarm will display a flashing border around their edge, which is coloured to match the alarm priorities displayed on the [Alarms](#) page.

Hover the mouse cursor over a map item to see the name of that item, and click on it to either navigate to the linked map, or to bring up a menu of actions the Operator can perform for that device.

The menu of actions contains 4 distinct segments, in order from top to bottom:

1. Item name (always present and visible)

2. Alarm details (only present when an alarm exists for that device and the Operator has appropriate permissions)

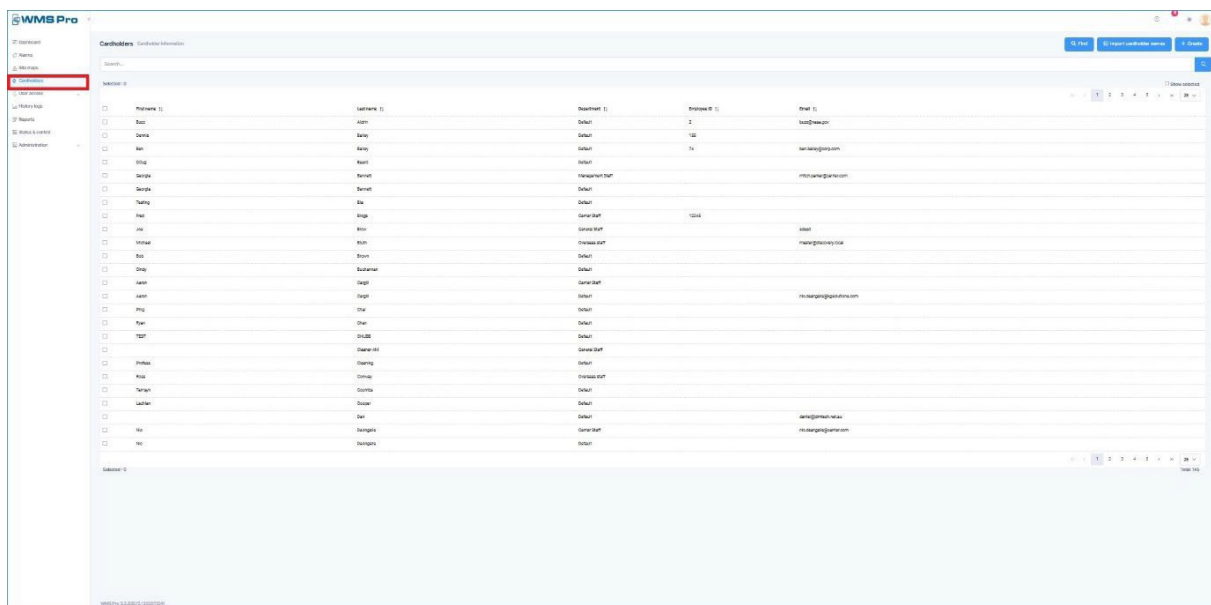
3. Other maps the device has been placed on (only present when a device is on more than one map and the Operator has appropriate permissions)

4. Device commands (visibility of each command is controlled by the device permissions set for the [Status & control](#) page for each Operator and/or Role)

Click on any item(s) within these segments (except for the first showing the item name) to perform the relevant action, such as responding to an alarm, navigating to another map, or sending a command to the device. Any action(s) taken will be logged as a History event, which may be visible within the Recent history widget on the [Dashboard](#) page, the [History logs](#) page, etc.

Cardholders

Cardholder information



Cardholders are the equivalent to users that are stored in the Controllers. When the initial configurations are retrieved from the Controllers, the user information is also transferred to WMS Pro.

Search bar

Enter a search term to narrow down the Cardholder list to assist with locating a specific profile.

Find

By controller user

Select the Controller and enter the User number to find the desired Cardholder.

By credential details

Select the Card format of the credential, then enter the appropriate details in the given fields. Press the **Find** button, if the credential exists, then the page will be redirected to the matching Cardholder record.

Import cardholder names

Cardholder names in WMS Pro can be replaced by matching a first/last name with Raw card data or card format details. By importing a CSV file containing a list of names and corresponding credential details, WMS Pro will update Cardholder names which match credential details.

Click [here](#) to download a sample CSV file, or refer to the example provided below:

First name	Lastname	Raw card data	Card format	Site code	Card number
John	Doe	27.0.0.0.222.39.99			
Jane	May		Tecom 27 bit	10	24

The table above is an example of what the format should look like in the CSV file. WMS Pro will either look at the Raw card data or the Card format, Sitecode, and Card number to match the Cardholders. Using the example above, if there is a Cardholder with a Credential containing the Raw card data of 27.0.0.0.222.39.99, then that Cardholder's name will be changed to John Doe.

Note: In the Card format field, the Card format name needs to match the name shown in the [Credential group](#) Card format selection list.

Once the file has been imported, a "Imported Cardholders" file will be downloaded. This file will contain a list of all the old names and the new names that have replaced it.

Cardholders can have their details edited by clicking on their name.

Cardholders can be deleted by hovering over a Cardholder's name and clicking on the  symbol. They can also be deleted in bulk by ticking multiple checkboxes next to their first name and then clicking on the  symbol on the bottom right.

Create/Edit Cardholder

For existing Cardholders, clicking on the < and > icons will navigate to the next Cardholder in the list.

User details

Cardholder details such as **name**, **email address** and **employee ID** can be configured here.

Profile picture

A profile picture for the Cardholder can be uploaded by clicking on the + symbol underneath the portrait. To remove the profile picture click on the — symbol.

Department

[Departments](#) can be created in WMS Pro and assigned to Cardholders. The Department chosen also determines the [Custom fields](#) that appear in this tab.

Access groups

Assigning Controller Access Group (CAG)

In the Access group tab there will be a list of [Controllers](#) and there will be a  symbol on the same row as these Controllers. Clicking on the  symbol will open a pop up window that contains all the CAGs available for said Controller, the Operator can assign these CAGs to the Cardholder.

Clicking on the actual CAG name will expand that row and displays the **Alarm**, **Door**, and **Floor** information. Click on the  icon next to the Alarm/Door/Floor group to open a new pop-up window that contains "read-only" information for the group.

 **Alarm group details:** the alarm group's setup, options and menus information is displayed in this window

Setup: displays the permissions approved for arming, disarming, alarm reset, and timing for the assigned Areas. **Options:** additional settings for the alarm groups. **Menus:** user function available (via an LCD RAS) to Cardholders with this alarm group.

For more information on the options and menu, see the [Controller Access Groups](#) page.

 **Door/Floor group details:** provides information on the [Timezones](#) allocated to the Door/Floor. In the details column click the "more" button to expand the row, click on the  icon to change the Timezone view to a Timezone grid.

Assigning Unified Access Group (UAG)

Tick the **Unified Access Group** check box at the top of the page to select any existing UAG. To create UAGs on the fly, make sure the **Unified Access Group** check box is unticked and the

Cardholder has been assigned at least one CAG. The [Operator](#) should then be able to click the "Create" button. A prompt will then appear to name the new UAG.

Credentials

Click on any existing Credentials to expand the row and view the **Site code**, the **Raw Card data**, and the Start and End date. At the end of the line entry hover mouse to reveal icons for: Write card, and Edit Credential.

Create/Edit credential(s)

Make sure to create at least one [Credential group](#) before creating a new Credential for the Cardholder.

 Create: Click this icon on the bottom left to add a new Credential to the Cardholder's profile. A new pop up window will appear.

 Assign: Click this icon to display a list of unassigned Credentials to select from.

 Delete: To delete Credentials, tick the checkbox next to the Credential name and then click on the  icon on the bottom left.

When a Credential is created the popout box will display 3 tabs, that being:

Card details

Pin only (checkbox)

Check the **Pin only** checkbox to make the cardholder credential have a PIN only credential. This will set Credential group to 'Auto generate PinOnly'. Zero card data will be saved against the Credential.

Credential group

Select the desired [Credential group](#), the group chosen determines which [Controller](#) the Cardholder's details get sent to.

Card format

The card format attached to the chosen Credential group will automatically populate this field. This field cannot be modified manually.

Name

Name of the Credential.

Site code

Enter the site code in this field if applicable (and if the Card format is not Raw card data).

Card data

The raw card data. There are seven segments, of which the first bit gives the total number of bits used. The other segments are typically calculated using the card number, site, and facility code.

This field is read-only unless the card format is **raw card data**.

Dates & Status

Start date/End date

Timeframe the Credentials are valid for. The Cardholder will be active after the start date and deactivated past the end date.

User type

Normal This only applies when connected to an intelligent Door Controller. Otherwise, the user type is Normal.

Dual custody Requires a second valid user PIN/card to be entered to perform any Alarm or access control functions.

Guard User's PIN/card can only perform functions when used in conjunction with a visitor's PIN/card.

Visitor Requires a PIN/card from a user who has the Guard card type. See above.

Status

Normal means that the credential will provide access to the Cardholder,

Void means that the credentials still exist in the system, but does not grant access for the Cardholder.

Expired means that the credentials still exist in the system, but does not grant access for the Cardholder.

Pending means that the credentials still exists in the system, but does not grant access for the Cardholder. It is waiting for the start date to become valid. Once start date is valid, the credential is sent to the controller(s).

Tick boxes consist of:

Card only

The user will NOT be able to use the PIN associated with a credential.

Extended access

The user will be allowed extended Door access times. For example, to allow a longer Door opening time for those who require it.

Trace

All Alarm and access functions performed by the user will cause a "Trace" message to be sent to the management computer.

Privileged

A user with a privileged setting has special permissions at Door Controller readers:

The user cannot be locked out by anti-passback settings (regions 0 to 199). The user can pass between regions without restriction. The user cannot be locked out by the 'Door reader disabled' macro event. The user can operate a reader that is disabled for other (non-privileged) users.

High security user

This option only applies to Network Access Controller Doors. A user with this option enabled will be able to access High security regions on Network Access Controller Doors (when configured).

Clicking on the  symbol will display a list of Controllers and the user slot the Cardholder has occupied in each of them.

PINs

Enter **PIN** and re-enter to **Verify**. Use **Show PIN** to verify input.

Select either: **Apply PIN to all controllers**, **Remove PIN to all controllers** or use the **Search** to locate the controller to assign the PIN to.

Once PIN is assigned it will display in a list with the following headings:

Name, Site, Serial number and Has PIN.

(Has PIN has either True or False. True means there is a PIN assigned to the controller)

The columns to the right of 'Has PIN' has buttons to: **Set PIN**, **Remove PIN**, and **View PIN**. (View PIN is only visible if the option is enabled in Settings and in the Operator's Permissions is set to 'View saved PIN' in the Credentials branch).

Note: This table will only show Controllers that the Cardholder has access to (CAG).

Note: PIN codes are verified against other PIN codes in the same **Controller** to ensure there are no duplicates in the system. If so WMS Pro will display that the PIN wasn't able to be set on

that Controller.

Programming Credentials into a Tecom smart card

If the Cardholder's Credential has the card format "**Tecom 27 bit**" then the  icon will be visible for the Cardholder.

Clicking on the icon will bring up a new pop-up window that will prompt the Operator to choose a Card programmer. Once it has been selected a smart card can be placed on the programmer to have the Cardholder's Credentials programmed into it.

Note: SCPInterface needs to be active for the Card programming process to occur, see [Card programmer](#) for more information.

Regions assigned

[Regions](#) are used to group Cardholders to ensure that they only have access to the Region they have been assigned to. The use of Regions also determines which Cardholder is visible or invisible to the [Operators](#).

This tab lists out Regions that have been assigned to the Cardholder. Pressing the  Assign button will open up a list of Regions that can be assigned to the Cardholder. Ticking the checkbox next to the Region name will cause the  icon to appear, press it to unassign the Region from the Cardholder.

Cardholders by default are assigned to the "System Default Region". All Cardholders must always belong to at least one Region, if they have been unassigned from all Regions they will be automatically reassigned to the System Default Region.

Events

Provides a list of most recent events provided by the Controllers in regard to the Cardholder.

Clicking on the "**Click here to browse for more events**" text will take the Operator to the [history logs](#) page with the Cardholder's name prefilled in the advanced filters.

Notes

An area for free text notes available in this area. These can be used as a reminder.

Print Preview

Click on the Print Preview to see the Cardholder's Photo ID. Both the front side and back side of the card can be previewed and printed. Buttons to Print the card and close the print preview are at the bottom of the page.

Notes:

- Cardholder must be assigned to a Department that has a card designed.
 - When changing Departments, operator must save record before print card will show the correct preview.
 - Print preview may show wrong size if card printer is not selected with appropriate page size for cards.
-

Copy Cardholder

In the **Edit Cardholder** page there is a **Copy** button in the top right of the page. Clicking it will

replicate the current Cardholder profile.

Create Cardholder

Next button is **Create**, where a new Cardholder can be created.

Delete Cardholder

The last button is the **Delete**, to delete the Cardholder record.

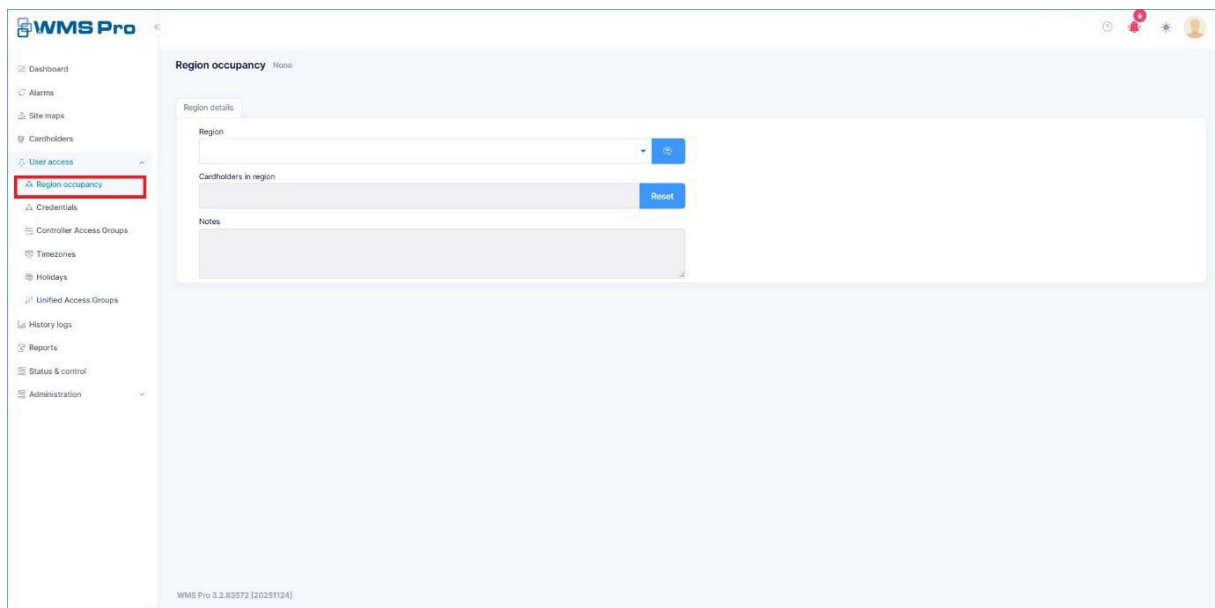
Granting access to a Cardholder

For Cardholders to gain access to a Controller, they will need to be assigned two things:

- Controller access group: this will give the Cardholder an Alarm/Door/Floor group for the chosen Controller.
- Credentials: creating a Credential requires a Credential group to be allocated to it. If a Cardholder shares the same Credential group as a Controller, then it's information is sent to that Controller.

Controllers are automatically assigned Credential groups during the enrolment process, and assigned Credential groups may be modified in the Controllers page under the Administration menu. This ensures that Credentials are only sent to a Controller when the Cardholder has both access and a valid Credential.

Region occupancy



Region occupancy shows how many cardholders are currently occupying a region. Active cardholders tab will show you which cardholders are occupying this region and when they accessed it.

Accessing a region's ingress device (door/lift/RAS/reader) will put a cardholder into that region. Accessing a region's egress device will remove the cardholder from that region.

On the 'Region details' tab you need to click on the Region drop down arrow to select the Region you need to view. Or click on the blue icon next to this to 'Select - Region'.

On the 'Cardholders in region' it will display the number of Cardholders in the selected region. You can Refresh the list by clicking on the 'Refresh' button and 'Reset' this list to zero cardholders.

Below this is an area to display 'Notes'. These are read only, and will show the stored Notes against the Region in the Regions page.

On the 'Active cardholders' tab there is a 'Search' bar where you can type in a Cardholders name. The results will then list out the Cardholder's information in the order of:

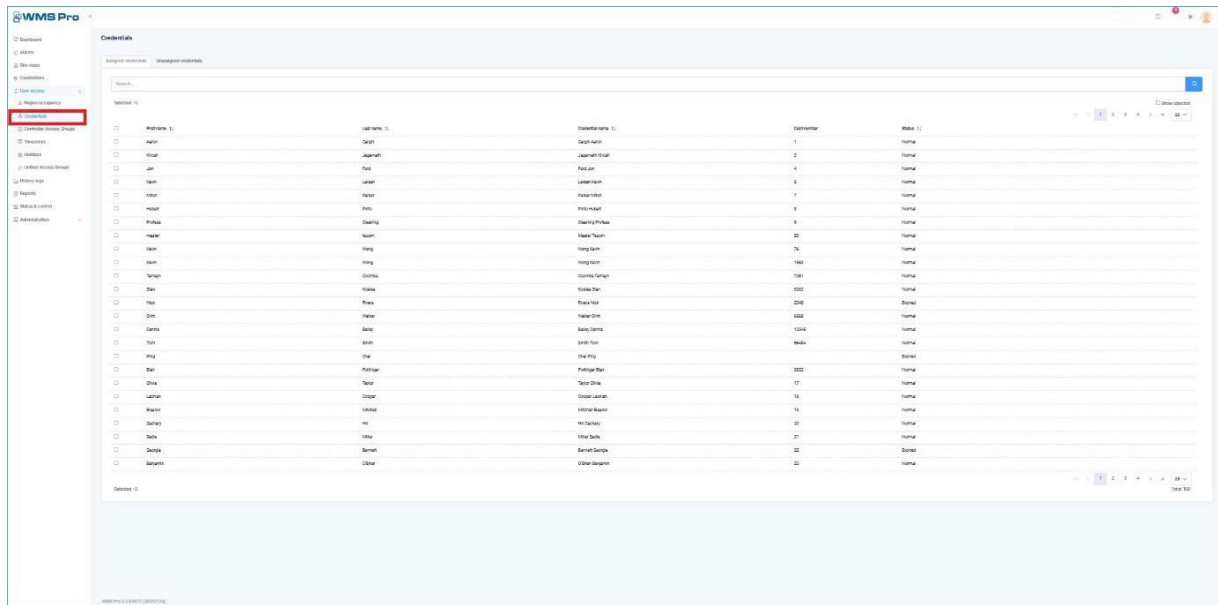
'First name', 'Last name' and 'Date time entered' (Device time, not system time).

With this list you then can either 'Export to PDF' or 'Export to Excel'.

The last button is to 'Delete all'. When you click on this it will ask you: 'Are you sure?'

Region Occupancy Reports can be generated in the Reports section of WMS Pro.

Credentials



Assigned credentials

Assigned credentials (displays a list of all Credentials currently assigned to Cardholders).

Click row to view/edit

Edit credential details as follows:

Credential group use the drop down, or search and select, option to select the Credential group.

Card format is self-populated from the Credential group.

Name: enter Credential name.

Start date & End date: Enter a Start and End date and time using the Calendar and time scale. Any dates in the future will have the Status of '[Pending]'.

User type drop down options:

- Normal
- Dual custody
- Guard
- Visitor

Status drop down options:

- Normal
- Void
- Expired

Site code: Enter site code

Card number: Enter card number

Card data: Is the data assign to the card that consists of a choices from above fields in a number code.

Check boxes: Tick the following checkboxes for:

- Card only
- Extended access
- Trace
- Privileged
- High security user

Save the Edit credential page.

Click  to Assign

Click icon to assign Cardholder to the Assigned credential

Click  to Unassign

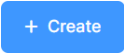
Click icon to unassign credentials.

Click  to go to the assigned Cardholder details

Once clicked the page will re-direct to the Edit Cardholder > Credentials entries of the Cardholder page.

Unassigned credentials

Unassigned credentials (displays a list of all Credentials not currently assigned to Cardholders).

 Create

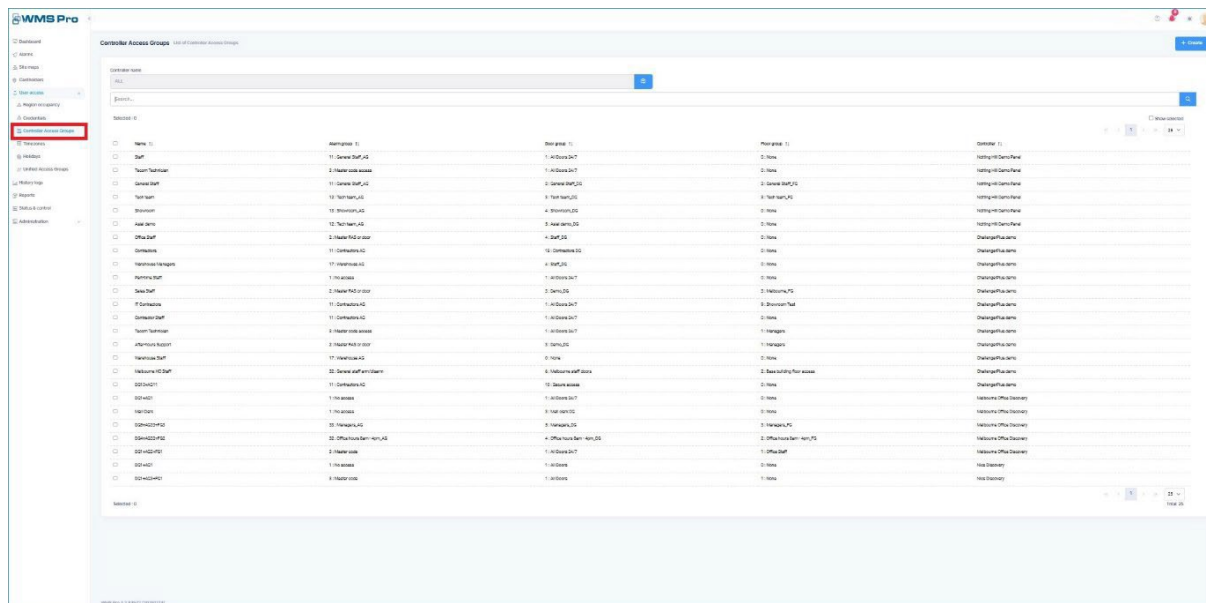
Create one or multiple Credentials using a common Credential group, card format, site code, start card number (and optionally quantity).

Click row to **view/edit** Credential as above.

Click  icon to Assign Cardholder to the Credential.

Controller Access Groups

List of Controller Access Groups



Name	Alarm group	Door group	Floor group	Region
Test CAG	1. Test Alarm	1. Test Door	1. Test Floor	1. Test Region
Test CAG 2	2. Test Alarm	2. Test Door	2. Test Floor	2. Test Region
Test CAG 3	3. Test Alarm	3. Test Door	3. Test Floor	3. Test Region
Test CAG 4	4. Test Alarm	4. Test Door	4. Test Floor	4. Test Region
Test CAG 5	5. Test Alarm	5. Test Door	5. Test Floor	5. Test Region
Test CAG 6	6. Test Alarm	6. Test Door	6. Test Floor	6. Test Region
Test CAG 7	7. Test Alarm	7. Test Door	7. Test Floor	7. Test Region
Test CAG 8	8. Test Alarm	8. Test Door	8. Test Floor	8. Test Region
Test CAG 9	9. Test Alarm	9. Test Door	9. Test Floor	9. Test Region
Test CAG 10	10. Test Alarm	10. Test Door	10. Test Floor	10. Test Region
Test CAG 11	11. Test Alarm	11. Test Door	11. Test Floor	11. Test Region
Test CAG 12	12. Test Alarm	12. Test Door	12. Test Floor	12. Test Region
Test CAG 13	13. Test Alarm	13. Test Door	13. Test Floor	13. Test Region
Test CAG 14	14. Test Alarm	14. Test Door	14. Test Floor	14. Test Region
Test CAG 15	15. Test Alarm	15. Test Door	15. Test Floor	15. Test Region
Test CAG 16	16. Test Alarm	16. Test Door	16. Test Floor	16. Test Region
Test CAG 17	17. Test Alarm	17. Test Door	17. Test Floor	17. Test Region
Test CAG 18	18. Test Alarm	18. Test Door	18. Test Floor	18. Test Region
Test CAG 19	19. Test Alarm	19. Test Door	19. Test Floor	19. Test Region
Test CAG 20	20. Test Alarm	20. Test Door	20. Test Floor	20. Test Region
Test CAG 21	21. Test Alarm	21. Test Door	21. Test Floor	21. Test Region
Test CAG 22	22. Test Alarm	22. Test Door	22. Test Floor	22. Test Region
Test CAG 23	23. Test Alarm	23. Test Door	23. Test Floor	23. Test Region
Test CAG 24	24. Test Alarm	24. Test Door	24. Test Floor	24. Test Region
Test CAG 25	25. Test Alarm	25. Test Door	25. Test Floor	25. Test Region
Test CAG 26	26. Test Alarm	26. Test Door	26. Test Floor	26. Test Region
Test CAG 27	27. Test Alarm	27. Test Door	27. Test Floor	27. Test Region
Test CAG 28	28. Test Alarm	28. Test Door	28. Test Floor	28. Test Region
Test CAG 29	29. Test Alarm	29. Test Door	29. Test Floor	29. Test Region
Test CAG 30	30. Test Alarm	30. Test Door	30. Test Floor	30. Test Region
Test CAG 31	31. Test Alarm	31. Test Door	31. Test Floor	31. Test Region
Test CAG 32	32. Test Alarm	32. Test Door	32. Test Floor	32. Test Region
Test CAG 33	33. Test Alarm	33. Test Door	33. Test Floor	33. Test Region
Test CAG 34	34. Test Alarm	34. Test Door	34. Test Floor	34. Test Region
Test CAG 35	35. Test Alarm	35. Test Door	35. Test Floor	35. Test Region
Test CAG 36	36. Test Alarm	36. Test Door	36. Test Floor	36. Test Region
Test CAG 37	37. Test Alarm	37. Test Door	37. Test Floor	37. Test Region
Test CAG 38	38. Test Alarm	38. Test Door	38. Test Floor	38. Test Region
Test CAG 39	39. Test Alarm	39. Test Door	39. Test Floor	39. Test Region
Test CAG 40	40. Test Alarm	40. Test Door	40. Test Floor	40. Test Region
Test CAG 41	41. Test Alarm	41. Test Door	41. Test Floor	41. Test Region
Test CAG 42	42. Test Alarm	42. Test Door	42. Test Floor	42. Test Region
Test CAG 43	43. Test Alarm	43. Test Door	43. Test Floor	43. Test Region
Test CAG 44	44. Test Alarm	44. Test Door	44. Test Floor	44. Test Region
Test CAG 45	45. Test Alarm	45. Test Door	45. Test Floor	45. Test Region
Test CAG 46	46. Test Alarm	46. Test Door	46. Test Floor	46. Test Region
Test CAG 47	47. Test Alarm	47. Test Door	47. Test Floor	47. Test Region
Test CAG 48	48. Test Alarm	48. Test Door	48. Test Floor	48. Test Region
Test CAG 49	49. Test Alarm	49. Test Door	49. Test Floor	49. Test Region
Test CAG 50	50. Test Alarm	50. Test Door	50. Test Floor	50. Test Region

Controller Access Groups (CAG) are a combination of a user's Alarm group, Door group and Floor group. They are automatically generated when a **Controller** is enrolled in WMS Pro.

A unique CAG is created for every unique combination of Alarm, Door and Floor groups assigned to each user found in the enrolled Controller. CAGs can be assigned to **Cardholders** in WMS Pro and also be created in the Controller Access Groups page.

Note: Duplicate CAGs (either name or configuration) are not allowed in WMS Pro.

Controller name

Clicking on the  icon next to the Controller name will open a new pop up window and allow you to select a Controller and filter the CAG list based off the chosen Controller.

Search bar

Enter a search term to narrow down the CAG list to assist with locating a specific CAG. Search results can be limited to CAGs assigned to a specific Controller by clicking on the "Controller name" drop down menu and selecting the desired Controller.

CAG can be edited by clicking on their name.

They can be deleted by hovering over the CAG name and clicking on the  symbol. They can also be deleted in bulk by ticking multiple checkboxes next to the CAG name and then clicking on the  symbol on the bottom right.

Edit CAG

Once a CAG entry has been clicked on it will open up the Edit CAG page which has 3 tabs: CAG, details, Assigned cardholders, and UAG cardholders.

CAG details

Here is where the **Name**, **Alarm group**, **Door group**, **Floor group**, and **Region** can be edited.

For the Alarm group, Door group, Floor group, and Region, use the drop down or search button to choose the option needed.

Click the  icon to see the Group finer details to tick as further option. Use the  icon to add a new Group. Once all choices have been selected **Save** the CAG details.

Assigned cardholders

Use the  icon or locate the Cardholders to Assign from the list. Tick to select and click the  to assign the cardholder to the CAG. The  button will unassign the Cardholder from the CAG.

UAG cardholders

Use the  icon or locate the Cardholder(s) assigned to this CAG via a UAG.

Create

If you haven't selected a specific Controller yet from the Controller drop-down menu, you will be prompted to choose one. Once a Controller has been chosen, there will be two options provided to determine the CAG creation process, **Wizard** and **Classic**.

Note: The options that the Operator can choose from depends on the Controller they selected. For example, if Controller 1 was selected, only Door groups found in that Controller will be visible in the creation page.

Wizard

The Wizard process provides a "broad stroke" method of creating CAGs; however you still have the ability to make small granular changes later on in the edit page.

Name

CAG name.

Timezone

Select one of the [Timezones](#) that appears in the drop-down menu. Only the Timezones that have been assigned to your chosen Controller will be visible.

Note: The Timezone will be applied to all groups chosen, unique Timezones for each group can be done in the edit page for the CAGs.

Areas

Select the Areas from the list. Tick the checkbox next to the "Areas" to tick all the Areas in the list.

Note: Area groups may also be created alongside the other groups.

Doors

Select the Doors from the list. Tick the checkbox next to the "Doors" to tick all the Doors in the list.

Floors

Select the Floors from the list. Tick the checkbox next to the "Floors" to tick all the Floors in the list.

"Show configured" checkbox

You can tick the checkbox to hide all the unconfigured Areas, Doors or Floors in the Wizard set up mode.

Once CAG settings have been configured and you have clicked "**Next**", you will be taken to a summary page that displays the CAG name, all the selections made, and the Timezone.

Create (Classic)/Edit CAG

The Alarm, Door and Floor group can be selected by clicking on the group name and choosing the desired option from the drop-down menu.

Click the  icon to edit the chosen group, click the  icon to create a new group.

Name

CAG name.

Create/Edit alarm group

Alarm group name - Name of the alarm group

Timezone

This defines the [Timezone](#) applicable to this alarm group. Functions restricted/available via this alarm group will be applicable only for the periods allowed by the selected 'hard' panel Timezone or soft Timezone.

Make sure that Timezones have been assigned to the chosen Controller for them to be visible.

Alt alarm group

Each alarm group may have an alternate alarm group. These alarm groups are only used when the original alarm group records a Timezone with access times which are invalid when a function is attempted. If the Timezone of the original alarm group denies access, the alternate is checked.

Note: The alternate alarm group may also be programmed with an alternate alarm group and so on – up to three alarm groups (the original plus two alternates). If a function is denied by the Timezone of one alarm group, the next will be checked (and so on). In this way, opposing functions may be made available at different times, days, etc.

Areas

An alarm group can be linked to a single Area or to an Area group.

When linked to a single Area, the alarm group controls the Area's permissions for arming, disarming, alarm reset, and for timing. When linked to an Area group, the Area group controls each Area's permissions for arming, disarming, alarm reset, and for timing. Tick the check box for **Arm**, **Disarm**, **Reset** and **Timed** to enable those permissions for the Area/Area group.

- **Arm** - Tick this check box if the Area can be armed.
- **Disarm** - Tick this check box if the Area can be disarmed.
- **Reset** - Tick this check box if the Area can be reset.
- **Timed** - Tick this check box if the Area may be disarmed for a timed interval.
The **Disarm** check box must also be *Ticked*.

By selecting **Area Group** you will also have the ability to create new groups by clicking on the "Create" button.

Options

Remote access *Ticked* – UltraSync and modem access with VT100 terminal (or terminal emulation software) is allowed by a user with this alarm group. If using the VT100 terminal, RAS 16 must have a suitable alarm group assigned to specify functions available (for example, alarm group 2) and be programmed as an LCD RAS. The RAS does not need to be polled.

This option does not apply to system management software unless connecting over UltraSync.

Alarm system control *Ticked* – Alarm system control functions are allowed by a user with this alarm group; or at a Door or RAS with this alarm group. *Unticked* – No Alarm system control functions are

allowed. Access control functions and any user menu options specified are still valid. Alarm control functions are Arm, Disarm, Reset Alarm etc.

Note: As well as a *Ticked* setting for control of all Alarm system functions, this check box must be set to *Ticked* if any of the other Alarm system control function restrictions in the alarm group are set to *Ticked*.

Reset system alarms

System Alarms are conditions such as DGP Tamper, Siren Fail, Low Battery, Report Fail etc.

Ticked – Allows a user with this alarm group to reset the latching System Alarms. This is only valid if **System alarms latch** (on the Options tab of the System options form in **CTPlus**) has been *Ticked*.

Note: If this is *Ticked*, **Alarm system control** (above) must also be *Ticked*.

User alarm group *Ticked* – Allows the alarm group to be assigned to a user. *Unticked* – The alarm group cannot be assigned to a user.

Prompt with list of areas

This check box controls the way in which Areas are presented on an LCD during arm/disarm procedures.

Ticked – The Areas assigned to the user will be displayed (after entering a PIN and [ENTER]) to enable selection from arm/disarm options (specific Areas, all Areas etc.). This is useful where a user is capable of controlling a number of Areas but usually needs to arm/disarm specific Areas only. *Unticked* – The Areas assigned to the user will not be displayed. PIN and [ENTER] will immediately arm/disarm Areas when using the RAS.

Keypad duress

Ticked – The keyboard duress facility allows a code to be entered on a keypad to activate duress. *Unticked* – Duress cannot be activated. A duress code is treated as an invalid PIN.

Auto isolate

This field relates to the treatment of unsealed inputs during the arming procedure.

Ticked – If there are unsealed inputs when the arming procedure is instigated, those inputs will automatically be isolated and the system will be armed without causing an Alarm. *Unticked* – It will not be possible to arm the system when there are unsealed inputs (unless **Forced arming** (below) is ticked).

Forced arming

This field relates to the treatment of unsealed inputs during the arming procedure.

Ticked – The check for unsealed inputs is ignored and if there are unsealed inputs when the arming procedure is instigated, the system will still arm. The inputs will remain unsealed and, depending on the input type, may cause an Alarm. *Unticked* – It will not be possible to arm the system when there are unsealed inputs (unless **Auto isolate** (above) is ticked).

Note: See **Enable exit fault reporting** (on the Options tab of the System options form in **CTPlus**) to report Alarms from non-entry/exit type inputs as Exit Error Alarms.

Prevent forced disarming

This field relates to the treatment of unsealed inputs during the disarming procedure and may be used if there are Access Alarm input types such as Type 1 and Type 11 in the system.

Ticked – Area/s cannot be disarmed if there are unsealed inputs. *Unticked* – Area/s can be disarmed even if there are unsealed inputs.

No arming if category not timing

This field relates to user category functions. (Refer to Install Menu Option 15 for full information on user categories in **CTPlus**).

Ticked – If an Area has been disarmed and there is no user category timer running, it will not be possible for a user category timer to be started. (A user category timer, when expired, will arm an Area, so setting this option will prevent an Area being armed when it has originally been disarmed by a user without user category functions.) *Unticked* – Normal user category functions apply.

Disable auto de-isolate

Ticked – A user is prevented from automatically de-isolating inputs in the Area they disarm. Not applicable if **Auto de-isolate when Area accessed** (on the Options tab of the System options form in **CTPlus**) is *Unticked*. Used for cleaners etc. *Unticked* – A user can automatically de-isolate inputs in the Area they disarm.

Enable area search

When *Ticked*, a user with this alarm group must perform an Area search as part of the disarming process during a specified Timezone (the **Area search Timezone** programmed on the Setup tab of the System options form in **CTPlus**).

User categories 1 to 8

If multiple user categories are assigned to an alarm group, then the lowest user category number applies. Challenger functionality can depend on the alarm group assigned to a user, and the alarm group assigned to a RAS. In these cases, the lowest common user category number applies. For example, if a user has an alarm group containing user categories 3 and 4, and a RAS has an alarm group containing user categories 1, 2, 3, and 4, then only user category 3 would apply to that user at that RAS.

User categories 1 to 8 provide timing for an alarm group's Areas that are configured for timed disarming or for delayed arming via vault programming (see the Vaults form in **CTPlus**). The user category time is configured in Timers in **CTPlus**.

Ticked – The user category functions will be activated when a PIN is entered.

Menus

The Menus tab determines which user functions will be available (via an LCD RAS) to users with this alarm group, or on a RAS with this alarm group. Each user menu option is displayed and must be *Ticked* for it to be available to the alarm group (and therefore the user or RAS). The user options available for selection are summarised below.

No.	RAS Menu	Description
1	Panel Status	A user with this option enabled can list any inputs which are in Alarm, isolated or unsealed. There are menu options available which display each of these conditions separately, however, this option may be used to check on all inputs which need attention.
2	Input Unsealed	A user with this option enabled can see all unsealed inputs, for example, Door open. The function would be used to determine whether you need to check an input in order to maintain security. For example, close the Door.
3	Input In Alarm	A user with this option enabled can see details of all inputs which are in Alarm and tamper Alarm. Alarms should be acknowledged and reset.
4	Input Isolated	A user with this option enabled can see details of all isolated inputs. An isolated input is one which is excluded from functioning as part of the security system. It would be isolated because it is faulty or broken and by isolating it you would stop it causing an Alarm. This function would therefore be used to determine which inputs are not operational and need attention.
5	History	A user with this option enabled can see past events of system history, including Alarms, access to the menu etc. It can help you determine events such as time that an Alarm occurred, the time it was reset and who reset it,

		the time the system was disarmed in the morning etc. The events are displayed in reverse chronological order, i.e. the last event is the first shown.
6	Test Report	A user with this option enabled can see the results of the Secure Test which is done on specific inputs to see if they were operating correctly. The inputs are those that are programmed to be included in testing and which operate when a building is unoccupied.
7	Service Menu	A user with this option enabled can request a service call or to establish connection to a remote service centre to allow programming over the telephone network.
8	Film Counters	A user with this option enabled can see the current frame number position on each of the security camera films. If you maintain a log on frame counts it will indicate whether the cameras have operated since they were last checked.
9	Input Text	A user with this option enabled can see the text that is programmed as a description of the inputs in your system.
10	Isolate	A user with this option enabled can isolate inputs i.e. exclude them from functioning as part of the security system. An input would be isolated because it is faulty or broken and by isolating it, you would stop it causing an Alarm. The function provides a list of unsealed inputs for you to select an input to isolate. A faulty or broken input is usually unsealed; however, sealed inputs may also be isolated if you know the input number.
11	Deisolate	A user with this option enabled can de-isolate inputs, i.e. return them back to functioning as part of the security system. An input is isolated because it is faulty or broken and when it is repaired it must be de-isolated.
12	Test Input	A user with this option enabled can test an individual input device to determine if it is operating correctly.
13	Start Auto Access Test	A user with this option enabled can start the access test.
14	Program Users	A user with this option enabled can add, delete, or change a user. Your system may have been set up to require two authorised users to enter this menu.
15	Time & Date	A user with this option enabled can program a new time and date. The time and date are not visible during normal use of the Challenger; however, all internal functions are reliant on them. A new date or time would only need to be programmed when the Challenger is first installed or if the time needs to be adjusted for daylight saving. The time is programmed for a 24 hour clock.
16	Isolate/Deisolate RAS/DGP	A user with this option enabled can isolate or deisolate RASs and DGPs.
17	Enable/Disable Service Tech	A user with this option enabled can enable and disable the service technician's code. (Activates time zone 25 when service is enabled and deactivates time zone 25 when service is disabled).
18	Reset Camera	A user with this option enabled can reset the film frame count on a security camera to zero, or change the frame count number on an individual camera. This would be necessary when you change the film in the camera.
19	Install Menu	A user with this option enabled can access the Install Menu. Caution is to be taken over who is given access to this option.
20	Door and Floor Groups	A user with this option enabled can program Door and Floor groups.
21	Holidays	A user with this option enabled can record the date of Holidays. The Holidays recorded here may be used in conjunction with Timezones to control access (for example, staff who are allowed access during normal weekdays can be denied access on weekdays declared a Holiday). The Challenger is capable of recording up to 24 Holiday dates.
22	Open Door	A user with this option enabled can open a Door via an LCD RAS.

23	Unlock, Lock, Disable and Enable	A user with this option enabled can unlock, lock, disable, and enable a valid Door via an LCD RAS. Depending on the type of panel, the Door range this will work with may be different. For example: • ChallengerPlus: Doors 1-128 • ChallengerLEPlus: Doors 1-18
24	Automation Control	A user with this option enabled can manually control automation zones via LCD RAS.

Matching alarm groups

Contains a list of alarm groups that also contain the same Areas as the ones selected.

Create/Edit door and floor group

Tick the check boxes to select the desired Doors/Floors and allocate the appropriate Timezones for each of them.

Selecting a Door/Floor will also populate the **Matching Door/Floor group** with a list of Doors/Floor groups that contain said Door/Floor, which can be very useful in preventing duplicate groups from being created. Clicking on a matching group under the matching column will apply that group's settings on top of the current group. This will also apply the Timezone to the individual entities in the group. Multiple groups can be selected to have their settings applied to the current one.

Region

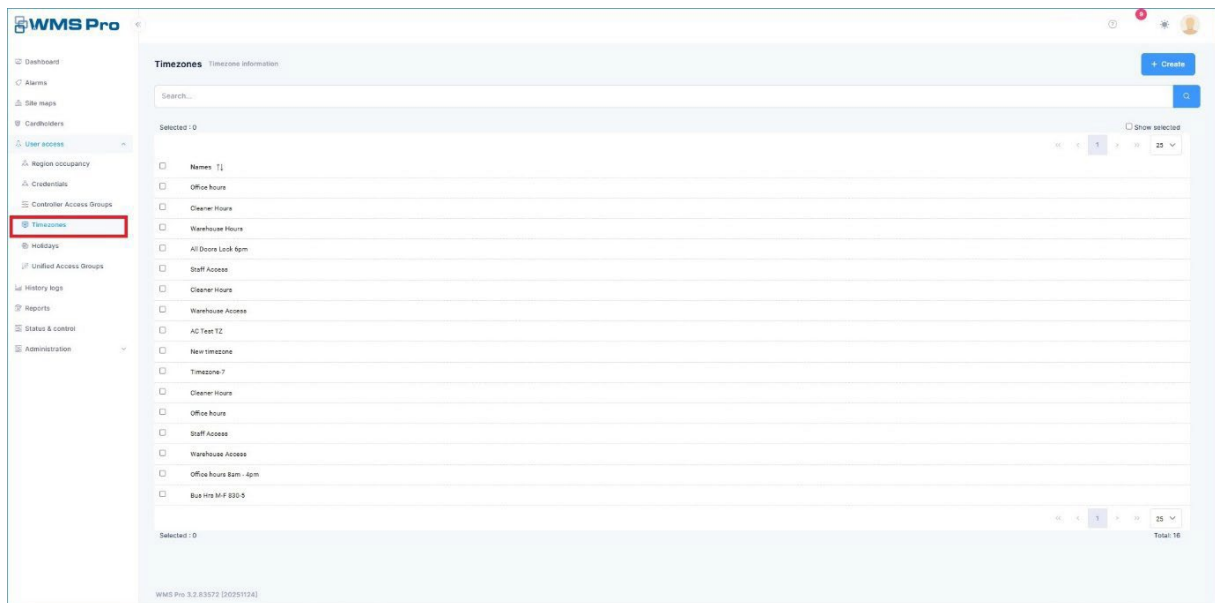
Click the dropdown arrow to select a 'Region.'

"Show configured" checkbox

You can tick the checkbox to hide all the unconfigured Areas, Doors or Floors in the Classic set up mode.

Timezones

Timezone information



Timezones define a period of time where **Controller** operations can be enabled or restricted.

Search bar

Enter a search term to narrow down the Timezone list to assist with locating a specific Timezone.

Timezones can be edited by clicking on their name.

They can be deleted by hovering over a Timezone's name and clicking on the  symbol. They can also be deleted in bulk by ticking multiple checkboxes next to the name and then clicking on the  symbol on the bottom right.

Create/Edit Timezone

Segments

Sub-timezones can be created in the grid by clicking and dragging from the top left to the bottom right of the desired shape. The dimensions of the shape can be modified by clicking and dragging the bottom right corner of the shape. The shape can be dragged and moved around the Timezone grid. A Timezone configured using this method will also appear in the list below with its own row and matching colour.

By clicking on the  button underneath the Timezone grid, Sub-timezones can also be defined by adjusting the start/end times and ticking the checkboxes of the associated days of the week.

Clicking on the checkbox on the left side of the Sub-timezone will select the whole Sub-timezone in the grid.

Name

Enter the name of the Timezone.

Region

Select a Region from the Drop down, or click on the blue icon to select a Region from a list.

Holiday type

The Holiday selection enables access to the Controller during Holidays. There can only be one Holiday type per Sub-timezone. One example on how to use this functionality is to have Holiday type 1 used for public holidays; when it is selected for the Sub-timezone the Controller will provide access during public holidays.

Visit the [Holidays](#) menu option page to create Holidays in WMS Pro. Holidays can also be assigned to Holiday types here.

Visit the [Holiday types](#) menu option page to rename the Holiday types.

Assigned Controllers

Timezones can be allocated to [Controllers](#) that are enrolled in WMS Pro. This is important as it allows you to assign Timezones to [CAGs](#) and Alarm/Door/Floor groups.

Pressing the  Assign button will open up a list of Controllers that the chosen Timezone can be assigned to. Ticking the checkbox next to the Controller name will cause the  icon to appear, press it to unassign the Timezone from the Controller.

Note: This tab is only visible in the edit page of the Timezone.

Holidays

Holiday information

Name	Start date	End date
☐ Christmas Eve	25/12/2023	25/12/2023
☐ New Year's Day	01/01/2024	01/01/2024
☐ Good Friday	06/04/2024	06/04/2024
☐ Easter	11/04/2024	11/04/2024
☐ May Day	01/05/2024	01/05/2024
☐ Bank Holiday	05/05/2024	05/05/2024
☐ Labour Day	01/09/2024	01/09/2024
☐ Christmas Eve	25/12/2023	25/12/2023
☐ New Year's Day	01/01/2024	01/01/2024
☐ Good Friday	06/04/2024	06/04/2024
☐ Easter	11/04/2024	11/04/2024
☐ May Day	01/05/2024	01/05/2024
☐ Bank Holiday	05/05/2024	05/05/2024
☐ Labour Day	01/09/2024	01/09/2024
☐ Christmas Eve	25/12/2023	25/12/2023
☐ New Year's Day	01/01/2024	01/01/2024
☐ Good Friday	06/04/2024	06/04/2024
☐ Easter	11/04/2024	11/04/2024
☐ May Day	01/05/2024	01/05/2024
☐ Bank Holiday	05/05/2024	05/05/2024
☐ Labour Day	01/09/2024	01/09/2024

A Holiday is a specified range of dates during which users are denied access during times that they would normally be permitted access. For example, a user may be able to disarm the system and unlock a Door during working hours except on defined Holidays.

Some users may require access during Holidays. This functionality is provided via a [Timezone](#) in a user's alarm group that has the relevant **Holiday type** selected.

Search bar

Enter a search term to narrow down the Holiday list to assist with locating a specific Holiday.

Holidays can be edited by clicking on their name.

They can be deleted by hovering over a Holiday's name and clicking on the  symbol. They can also be deleted in bulk by ticking multiple checkboxes next to their name and then clicking on the  symbol on the bottom right.

Create/Edit holiday

Name

Name of the Holiday.

Region

Use the drop down, or blue select region button to choose the Region. There is a Search option on this window as well to search for the Region.

Start date/End date

The time period of said Holiday.

Recurring

Tick the check box if the Holiday falls on the same date/s each year.

Holiday types

Assign the Holiday to the [Holiday type](#).

Holiday types are used to group Holidays together and provides greater flexibility in controlling access for users during Holidays. If a user's Timezone provides access on type 1 Holidays, any Holidays that are not type 1 are excluded (there can be 8 Holiday types).

Assigned Controllers

Select the [Controller](#) to assign the Holiday to, these Holidays will only apply to the chosen Controller.

Pressing the  Assign button will open up a list of Controllers that the chosen Holiday can be assigned to. Ticking the checkbox next to the Controller name will cause the  icon to appear, press it to unassign the Holiday from the Controller.

Note: This tab is only visible in the edit page of the Holiday.

Unified Access Groups

List of Unified Access Groups

[illegible]

Unified Access Groups (UAG) are a combination of multiple [Controller Access Groups](#) (CAGs) across multiple [Controllers](#). UAGs allow a single [Cardholder](#) to access multiple [Sites](#).

Search bar

Enter a search term to narrow down the UAG list to assist with locating a specific UAG.

UAGs can be edited by clicking on their name.

They can be deleted by hovering over a UAG name and clicking on the  symbol. They can also be deleted in bulk by ticking multiple checkboxes next to their name and then clicking on the  symbol on the bottom right.

Create/Edit UAG

UAG details

Name

Name of the UAG

Description

Description of the UAG

Region

Click the dropdown arrow to select a 'Region'.

Assigned access groups

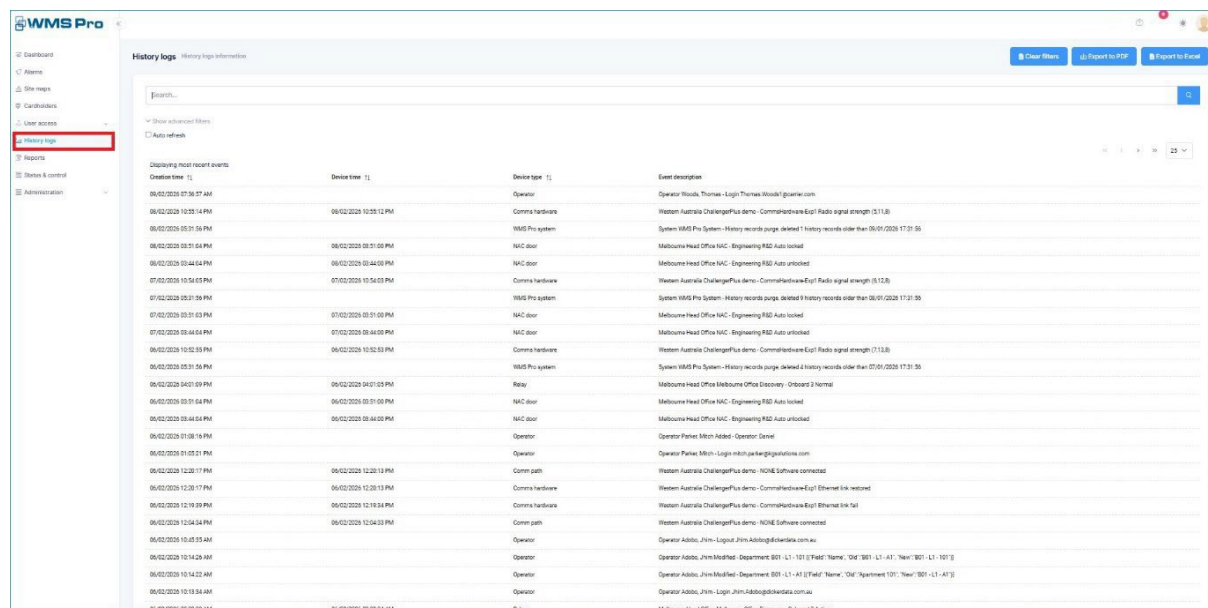
CAGs can be selected and grouped into the UAG through the **Controller** list. Click on the **P** symbol on the right side of the page. A pop-up window will appear with a list of CAGs attached to the Controller. Only one CAG can be chosen per Controller.

Assigned cardholders

Pressing the  Assign button will open up a list of Cardholders that can be assigned to the UAG. Ticking the checkbox next to the Cardholder name will cause the  icon to appear, press it to unassign the Cardholder from the UAG.

History logs

History logs information



Date/Time	Device type	Event description
06/02/2023 07:36:27 AM	Operator	Operator Woods, Thomas - Login Thomas Woods@goerke.com
06/02/2023 10:25:14 PM	Comma hardware	Western Australia ChallengePlus demo - CommaHardwareExp Radio signal strength (511.8)
06/02/2023 05:21:56 PM	WMS Pro system	System WMS Pro System - History records purge deleted 1 history records older than 06/01/2023 17:21:56
06/02/2023 03:51:44 PM	NAC door	Melbourne Head Office NAC - Engineering R&D Auto locked
06/02/2023 03:44:44 PM	NAC door	Melbourne Head Office NAC - Engineering R&D Auto unlocked
07/02/2023 10:54:03 PM	Comma hardware	Western Australia ChallengePlus demo - CommaHardwareExp Radio signal strength (512.8)
07/02/2023 03:51:44 PM	WMS Pro system	System WMS Pro System - History records purge deleted 1 history records older than 06/01/2023 17:21:56
07/02/2023 03:51:44 PM	NAC door	Melbourne Head Office NAC - Engineering R&D Auto locked
07/02/2023 03:44:44 PM	NAC door	Melbourne Head Office NAC - Engineering R&D Auto unlocked
06/02/2023 10:52:53 PM	Comma hardware	Western Australia ChallengePlus demo - CommaHardwareExp Radio signal strength (713.8)
06/02/2023 05:21:56 PM	WMS Pro system	System WMS Pro System - History records purge deleted 1 history records older than 07/01/2023 17:21:56
06/02/2023 04:01:02 PM	Relay	Melbourne Head Office Melbourne Office Directory - Onboard 2 Normal
06/02/2023 03:51:44 PM	NAC door	Melbourne Head Office NAC - Engineering R&D Auto locked
06/02/2023 03:44:44 PM	NAC door	Melbourne Head Office NAC - Engineering R&D Auto unlocked
06/02/2023 01:58:16 PM	Operator	Operator Parker Mitch Added - Operator Daniel
06/02/2023 01:02:21 PM	Operator	Operator Parker Mitch - Login mitch.parker@goerke.com
06/02/2023 12:20:17 PM	Comma path	Western Australia ChallengePlus demo - NOME Software connected
06/02/2023 12:20:17 PM	Comma hardware	Western Australia ChallengePlus demo - CommaHardwareExp Ethernet link restored
06/02/2023 12:19:39 PM	Comma hardware	Western Australia ChallengePlus demo - CommaHardwareExp Ethernet link full
06/02/2023 12:04:34 PM	Comma path	Western Australia ChallengePlus demo - NOME Software connected
06/02/2023 10:45:33 AM	Operator	Operator Adkins, Jhm - Logout Jhm.Adkins@data.com.au
06/02/2023 10:14:28 AM	Operator	Operator Adkins, Jhm Modified: Department 801 - L1 - 101 (Floor) Name: 'DM' 801 - L1 - AT: 'New' 801 - L1 - 101 (Floor)
06/02/2023 10:14:22 AM	Operator	Operator Adkins, Jhm Modified: Department 801 - L1 - AT (Floor) Name: 'DM' Apartment 101: 'New' 801 - L1 - AT (Floor)
06/02/2023 10:13:48 AM	Operator	Operator Adkins, Jhm - Login Jhm.Adkins@data.com.au
06/02/2023 08:08:28 AM	Relay	Melbourne Head Office Melbourne Office Directory - Onboard 2 Notice

The history logs will show events for activities in both software and connected hardware. The search bar and advance filters can help the **Operator** find the specific events they are searching for.

For software events, the **Event description** will display who was responsible for the change, and the previous and current values.

Note: The maximum number of displayed events is capped at 1000. This applies to exported history logs as well. When going through the history logs **"Displaying first 1000 filtered events"** text will be displayed even when there are less than 1000 events.

Note: **Controller** events are associated with the hardware's device Region and not the Cardholder's Region.

Search bar

Events can be found by typing the event description into the search bar. Under the **Advanced filter** option, events can be filtered based on the start/end dates range, the device type in question, specific **Cardholder**, **Region**, and **Site**. Advanced filters now remember the state of the filter list after closing the page. On return to this page, the filters will be the same from earlier. Pressing the **Clear filters** button will reset/clear the remembered filters.

For high volumes of log entries (for example, more than 1000) it is advised to use the advanced filter function to reduce wait times.

Auto refresh

Tick the checkbox for the history logs to automatically refresh.

Export to PDF/ Excel

The history logs can be exported into a PDF file or Excel in the form of a history report.

Note: when exporting to PDF, the header page of the file will provide a summary of the filters applied to the report.

Reports

System reports

Customised filters can be generated for the [Operators](#) by using the in-built filters.

Report type

- Asset tracking report - used to track maintenance data of assets (Devices).
- Assigned credential report - this report shows a cardholder's assigned credential details.
- CAG summary report - reports on CAG's name with its Alarm groups, Door groups, and Floor groups listed.
- Cardholder access report - shows a cardholder's assigned UAG, CAG and assigned controller details.
- Cardholder device access report - shows a report with cardholders listed against devices that they have access to.
- Cardholder in CAG report - lists cardholders that have access to a device within the CAG.
 - Filters can be used to restrict results to:
 - All CAG's
 - All CAGs on a specific Controller only
 - A specific CAG on a specific Controller only
 - A specific group (alarm/door/floor)
- Cardholder in UAG report - a report to list Cardholder's names within a Unified Access Group.
- History report - lists out all event descriptions against a device's details and shows a date time of the occurrence.
- Inactive cardholder report - this report show how many days an Inactive cardholder has been inactive for, and expired cardholder's names.
- Region occupancy report - a report for a region's occupancy with cardholder's name and date time entered into that region.
- UAG summary report - used to show the UAG name, the controller it's assigned to and the assigned CAG name.

Output limit

By clicking the drop down arrow, you can have various options for the maximum number of entries within the generated report. These can be either:

- 1,000
- 5,000

- 10,000, or
- 20,000 entries

Device time filter

Ticking this box will apply the entered start/end times against the device time column instead of the systems time column.

Start/End date

The time frame of the report can be chosen by inputting the desired start and end times in the given field.

Filters

The Operator can filter out the report results by selecting the desired options found in the drop down menus.

Report template

Enter a 'Report template' name to store a collection of filters. This new report template can be used again as a quick action for commonly used reports.

Report format

By clicking the drop down you have options of PDF and Excel report formats to choose.

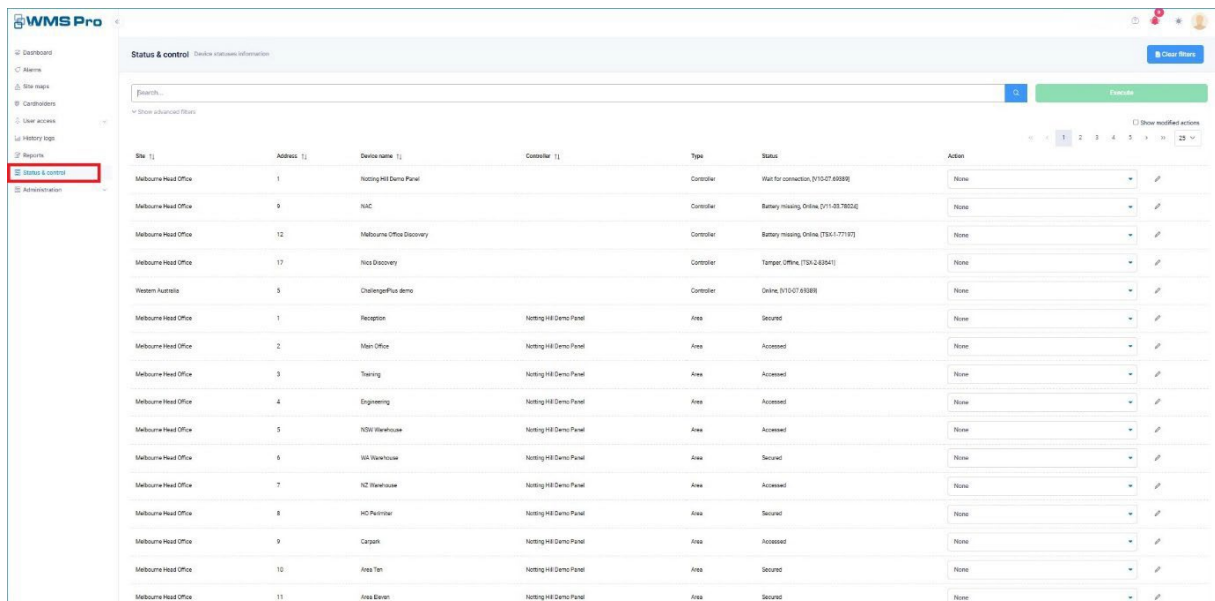
**Execute**

The execute button generates a report in either PDF or Excel file format. You can choose.

Note: The time format recorded in the generated reports may not match with what is recorded in the [history logs](#). This is due to the system's time format not matching. To fix the issue click on the Windows start bar and open **Control Panel > Region >** click on the **Administrative** tab > click on **Copy settings**. A new window will appear, tick the "Welcome screen and system accounts" and "New user accounts" checkboxes then click OK. The report's time format should now match with the history logs.

Status & control

Device statuses information



Site	Address	Device name	Controller	Type	Status	Action
Melbourne Head Office	1	Nothing M8 Demo Panel		Controller	Wait for connection (315-27-8888)	None
Melbourne Head Office	9	NSC		Controller	Battery missing Online (315-83-788342)	None
Melbourne Head Office	12	Melbourne Office Discovery		Controller	Battery missing Online (735-1-77187)	None
Melbourne Head Office	17	NSC Discovery		Controller	Tamper Offline (734-2-8341)	None
Western Australia	5	ChallengePlus demo		Controller	Online (315-27-8888)	None
Melbourne Head Office	1	Reception	Nothing M8 Demo Panel	Area	Secured	None
Melbourne Head Office	2	Main Office	Nothing M8 Demo Panel	Area	Accessed	None
Melbourne Head Office	3	Training	Nothing M8 Demo Panel	Area	Accessed	None
Melbourne Head Office	4	Engineering	Nothing M8 Demo Panel	Area	Accessed	None
Melbourne Head Office	5	NSC Warehouse	Nothing M8 Demo Panel	Area	Accessed	None
Melbourne Head Office	6	NSC Warehouse	Nothing M8 Demo Panel	Area	Secured	None
Melbourne Head Office	7	NSC Warehouse	Nothing M8 Demo Panel	Area	Accessed	None
Melbourne Head Office	8	NSC Warehouse	Nothing M8 Demo Panel	Area	Secured	None
Melbourne Head Office	9	Cargate	Nothing M8 Demo Panel	Area	Accessed	None
Melbourne Head Office	10	Area Ten	Nothing M8 Demo Panel	Area	Secured	None
Melbourne Head Office	11	Area Eleven	Nothing M8 Demo Panel	Area	Secured	None

Various commands can be sent to devices connected to WMS Pro on this page.

Search bar

Enter a search term to narrow down the list to assist with locating a specific device.

Execute button

Displays the number of actions pending, execution in brackets. Once pressed, the modified actions will be executed.

Show modified actions

Tick this checkbox to filter the device list to only show devices that have an **action** assigned to them. Devices with the **"None"** action assigned will not be visible as long as this checkbox is ticked.

Advanced filters

Devices can be narrowed down in the list by specifying the filters based on **device type**, **Region**, and **Site**. Advanced filters now remember the state of the filter list after closing the page. On return to this page, the filters will be the same from earlier. Pressing the **Clear filters** button will reset/clear the remembered filters.

Status filters

Allows the **Operator** to filter out what devices they want to look at.

The device must have the known status for it to appear in the Status filters field. If the status recall has not been completed for the device and/or change of state event has not been received for it, then the status of the device is unknown.

Favourites

Actions (see the section below) configured for a single or multiple devices can be saved as a preset for future repeated uses. Once the desired actions have been set for the devices, click on the **+** icon next to the favourites drop down list. A new pop up window will appear where the Operator will be prompted to name the favourite preset.

Favourites can be selected from the favourites drop down list, once selected they can also be deleted by clicking on the  icon.

Action

In the Action drop down menu are several commands that can be sent to the **Controller** remotely. **Multiple** devices can have an action be configured for them. Clicking on the  icon after selecting an action command will open a new window called "**Capture extra parameters data**".

Once the desired actions have been selected, click the **Execute** button to initiate the commands.

Note: For Doors/Lifts there are different command options based on the Door type selected. For example, if standard Doors are selected then the Operator is presented with **Standard doors Commands**. If a NAC Door was selected then the **NAC door Commands** is what appears in the **Action** drop down menu.

Activate / Deactivate service mode - By activating service mode on a controller a Technician can go in and carry out servicing or work as required. It is configurable with durations from the default as 60 minutes to the maximum at 720 minutes. Various warnings and statuses will appear:

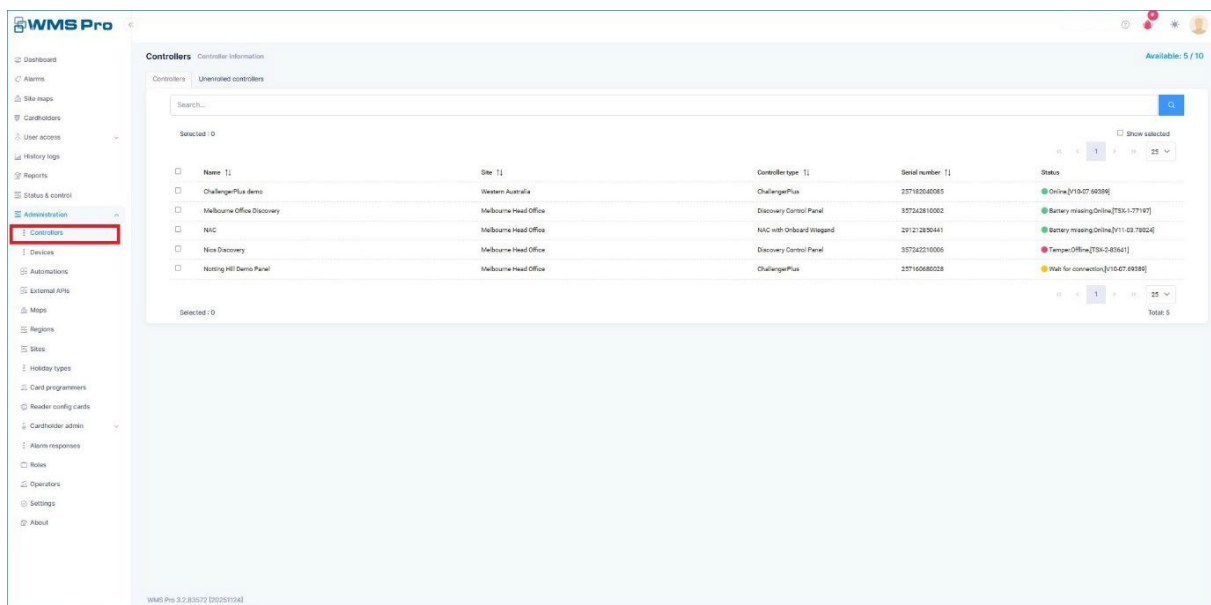
- Status column in Status & control page will indicate when it is 'In service mode'
- Maps - controller map items will also show these control commands and allow you to put it in or out of service mode
- Audit event is logged when controller is put in and out of service mode
- Status column in Controllers page will indicate when it is 'In service mode'. Controller row is highlighted in orange.
- Alarms generated from the controller while controller is 'In service mode' are logged as history events and no alarms are generated for these.
- When the controller goes out of service mode, WMS Pro performs an 'Update all device status.' Any alarms in controller are now raised as alarms in WMS Pro.
- Map controller icon goes orange when 'In service mode'
- 'In service mode' and 'Out service mode' can be used as triggers in an automation.
- 'Activate service mode' and 'Deactivate service mode' can be used as actions in an automation.

Capture extra parameters data

This option is different for each action; it allows the Operator to customise certain parameters of the chosen action. Send all and Retrieve all will have "All programming" assigned to it. If the parameters are left untouched the action will be executed with the default setting: "All programming". Change to this functionality is not required for typical operation. However you can change for "Cardholders" or "Installer only" configuration. For more information contact the technical support team.

Controllers

Controller information



Name	Site	Controller type	Serial number	Status
ChallengePlus demo	Western Australia	ChallengePlus	257163540065	Online (11/07/2016)
Melbourne Office Discovery	Melbourne Head Office	Discovery Control Panel	357322810002	Battery missing/Online (11/07/2016)
NAC	Melbourne Head Office	NAC with Onboard Wiigand	257121280441	Battery missing/Online (11/07/2016)
Nice Discovery	Melbourne Head Office	Discovery Control Panel	357322210006	Temporarily Offline (11/07/2016)
Nighting Hill Demo Panel	Melbourne Head Office	ChallengePlus	257160680028	Wait for connection (11/07/2016)

Controller information

A Controller is a device that connects to WMS Pro, such as the ChallengerPlus panel. Unenrolled Controllers are devices that have been configured to connect to WMS Pro, but have not been enrolled in the system.

The Controllers tab page contains a list of Controllers that have been enrolled in the system, clicking on their name will open up the edit page for that Controller. Any Controller that is in 'Service Mode' will have the line highlighted Orange. Controllers are put into 'Service Mode' from the Status and Control or Site Maps page.

On the top right side of the page, a count is displayed showing how many Controller licenses are available from the total number the installation is licensed for. This allows Operators to view how many Controllers may be added before an updated license is required.

Enrolling a Controller to WMS Pro for the first time

See the [quick start guide](#) for detailed instructions on enrolling a Controller to WMS Pro.

Search bar

Enter a search term to narrow down the Controller list to assist with locating a specific Controller.

They can be deleted by hovering over the Controller name and clicking on the  symbol. They can also be deleted in bulk by ticking multiple checkboxes next to their first name and then clicking on the  symbol on the bottom right.

Status

Each listed Controller will have its current status information displayed with an associated status colour on the rightmost column. The colour indicates the health of the connection the Controller has to WMS Pro.

Edit Controller

Setup

- **Name** - Panel Name.
- **Controller type** - The Controller panel being used.
- **Version number** - Shows Discovery panel version number. Non Discovery panels will show NA.
- **Identity** - Serial number of the control panel. It is a 12 digit number and is unique for every panel.
- **Communication type** - Refers to the communication method the Controller uses.
- **Location timezone** - Refers to the location Timezone the Controller uses.
- **Security password** - The security password is a 10-digit number that must match what has been programmed in the
- **Comms Path**. If the comms path is created using the wizard in CTPlus then the computer password can be specified by the installer.
- **Site** - WMS Pro [Site](#) assigned to the Controller. Click on the  icon to open up a new pop-up window with a list of Sites in the system.
- **Encryption key** - The encryption key is made up of digits and letters (i.e., alphanumeric text) and will be 32 characters in length. It is stored securely in WMS Pro and cannot be read, only changed. The key also changes periodically, being updated in both WMS Pro and the Controller, to ensure secure communication between them.

Note: The encryption key field needs to be identical to the encryption key used for the Controller. Clicking the auto generate button will create a new randomised encryption key.

- **Enabled** - Tick this checkbox to enable communication with the Controller.
- **Disable time synchronisation** - Check box is automatically configured and set to read-only when UltraSync is enabled and the Operator does not want WMS Pro to send commands to the panel to synchronise the time. Generally, when the Operator wants WMS Pro to be the secondary time synchronisation handler the check box should be ticked.
- **Migrate** - Press this button to migrate a ChallengerPlus panel into a Discovery V2 panel. (Only ChallengerPlus panels are applicable for the Migration to a Discovery V2 panel). Only V8 Door/Lift controllers need to be migrated to NAC's before migrating. The conversion will handle the migration of other Expanders.

Event configurations

The Event configurations tab will only be visible if the Alarm management functionality has been enabled for the WMS Pro [license](#) in use.

This page contains a list of possible events that can appear as an [Alarm](#) warning. The priority column displays the priority of the event, the lower the number the higher the priority. The highest priority event for the Controller will be the only one appear for that Controller in the Alarms list.

Clicking on the event name will open up a new pop-up window where the priority number can be configured.

To configure **multiple** events tick the checkboxes next to the names and press the  symbol on the bottom right of the list.

Holidays assigned

List of [Holidays](#) that are assigned to the Controller.

Timezones assigned

List of [Timezones](#) that are assigned to the Controller.

Regions assigned

Regions can be assigned to the Controller by clicking the '+ Assign' button.

Controllers by default are assigned to the "System Default Region". All Controllers must always belong to at least one Region, if they have been unassigned from all Regions they will be automatically reassigned to the System Default Region.

To manage the Region assignment of all devices, see the [Regions](#) page.

Credential groups assigned

A list of [Credential groups](#) will appear here. Clicking on the '+ Assign' button will assign the Credential Group to the Controller.

WMS Pro determines which Credentials belong to a Controller based on the Cardholder's CAG and Credential, and the assigned Credential Group(s) of each Controller.

Saving any changes made to this page will cause a full Cardholder sync to the Controller. All Cardholders with a CAG and matching Credential group will be downloaded to the Controller or deleted (if the Credential group is no longer assigned to the Controller).

Asset details

Device type: Enter the Device type of the control panel.

Last service: Enter the last service date of the panel.

Next service due: Enter the Next service due date of the panel.

Manufacturer*: Enter the panel's manufacturer. Eg: Tecom

Model / part number*: Enter the panel's Model / part number.

Description*: Enter a description for the Control panel.

Installed / serviced by*: Enter the name of who Installed / serviced the panel.

*These fields are required. Once details are entered click Save to update the Asset details.

Unenrolled Controllers / Network Access Controllers

To enroll a Controller or Network Access Controller, you must first use [CTPlus](#) to configure a WMS Pro comms path and save the changes (see the [quick start guide](#) for more detailed instructions). If done correctly the Controller / Network Access Controller will now appear in the unenrolled Controllers tabs. Click on the 'Control panel' drop down to choose either 'Control panel' or 'Network Access Controller'. You then need to click on the name, to open a new pop-up window called "Enrolling new Controllers".

Enrolling new Controllers / Network Access Controllers

- **Encryption key** - Enter the 6-digit encryption key generated by the CTPlus comm path wizard.
- **Site** - Enter a [Site](#) to assign to the Controller / NAC. For smaller sites, the default **System Default Site** should be fine.
- **Region** - Enter a [Region](#) to assign to the Controller / NAC. For smaller sites, the default **System Default Region** should be fine.

Once the changes have been saved, WMS Pro will attempt to communicate to the Controller using the specified encryption key. If successful, WMS Pro will automatically roll that key to a new randomly generated 32-character key and start the enrolment process, which will bring in all panel programming, construct [CAGs](#), and assign [Cardholders](#). This process may take several minutes depending on the size of the site. Once completed, the Operator will see a history log event saying "[Controller name] - Retrieve data complete", and the Controller is then ready to be used in WMS Pro.

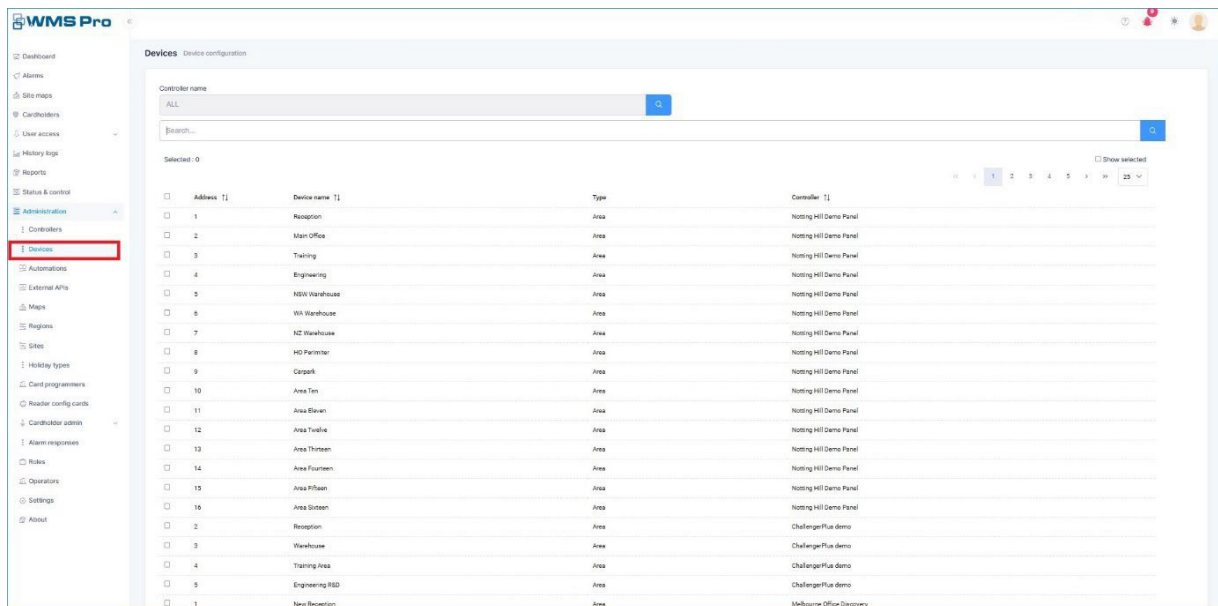
Once this has occurred the blue 'Available' number will change. For example, you could still have 3/5 Controllers available and 5/5 NAC's available to enroll on your WMS Pro license.

Note:

Attempting to connect to WMS Pro using CTPlus will fail if the fields found in CTPlus's **Panel programming -> Communications -> Comm paths -> Authentication** options contains any values.

Devices

Device configuration



This page contains a list of all the devices that can be found in the chosen [Controller](#).

Controller name

Clicking on the  icon next to the Controller name will open a new pop up window and allow you to select a Controller and filter the device list based off the chosen Controller.

Search bar

Enter a search term to narrow down the list to assist with locating a specific device.

Edit device

Click on the device name to be taken to its edit page.

Setup

The device name can be renamed here.

Note: When modifying the device name, the entire device configuration from when the Controller was enrolled or retrieved will be sent to the Controller.

Event configurations

Note: This tab will only be visible if the Alarm [license](#) has been applied to this version of WMS Pro.

The Event configurations tab contains all the events that can be generated by the device.

To edit the Alarm event you will need to click Menu > Administration > Devices. Select a Device, remember the Search feature can make it faster to locate. Click the "Event Configurations" tab. Locate the Event of interest and click it. This will then bring a box titled '**Edit event config**' up with the following fields:

Event text - You will see the 'Event text', this is the name of the one clicked.

Custom text - Is where you can change the 'Event text' name.

Priority - Each of these Alarm events will have an associated priority number next to them, the higher the number the lower the priority. The active alarm event with the highest priority (with the lowest priority number value) for a given device instance will be the event which will be highlighted in the Alarms list page under the Unacknowledged/Follow up tabs.

Next you will have the following **tick boxes**:

Alarm event

Tick the 'Alarm event' to change it to an Alarm event.

Output to API

Events that have 'Output to API' ticked will be sent to external devices that utilise the 3rd party API. Example: Reception Area has its secured event set to 'Output to API' but the Warehouse Area doesn't. Both areas are secured. When a 3rd Party integration performs a 'GetHistoryLog' API call, the response will include the Reception Area secured event, but it will not include the Warehouse Area secured event.

Persistent alarm

Persistent alarms require Operator attention. WMSPro will not automatically move the alarm to follow-up once it's been responded to, nor should it automatically remove the alarm from the list if the condition has been removed. It will require an Operator to manually delete the alarm. On the event configuration, 'Persistent alarm' needs to be set to True for that event on the device to become persistent.

Email on event

When 'Email on event' is ticked on the 'Edit event config', WMS Pro will automatically email specific [Operator\(s\)](#) when that event occurs. For this to function correctly, both 'Alarm event' and 'Email on event' must be ticked for each event to be emailed. The email is sent to Operators that have 'Email on event' ticked and share at least 1 Region with the Device.

Priority alarm overlay

'Alarm event' needs to also be ticked for this functionality to work. When the 'Priority alarm overlay' is ticked, WMS Pro will display the alarm to Operators using a priority overlay. The priority overlay will block out the Operator's screen until the alarm has been responded to, and is intended to ensure critical alarms are immediately visible and actioned urgently. This overlay may also be disabled per-Operator by ticking the 'Disable override alarm' option on the Operator's record.

You will then have options to 'Bulk save', 'Save', and 'Close'

Bulk save

'Bulk save' allows you to easily assign the same custom settings to other devices of this type. Example: It is a quick way to change the priority of the Secured event for all areas.

Regions assigned

Regions are used to group Devices to ensure that Operators only have access to the Regions they have been assigned to. Operators are unable to see Devices in Regions that are not assigned to them.

This tab lists out Regions that have been assigned to the Device. Pressing the  Assign button will open up a list of Regions that can be assigned to the Device. Ticking the checkbox next to the Region name will cause the  icon to appear, press it to unassign the Region from the Device. The maximum assigned Regions can be a total of 10.

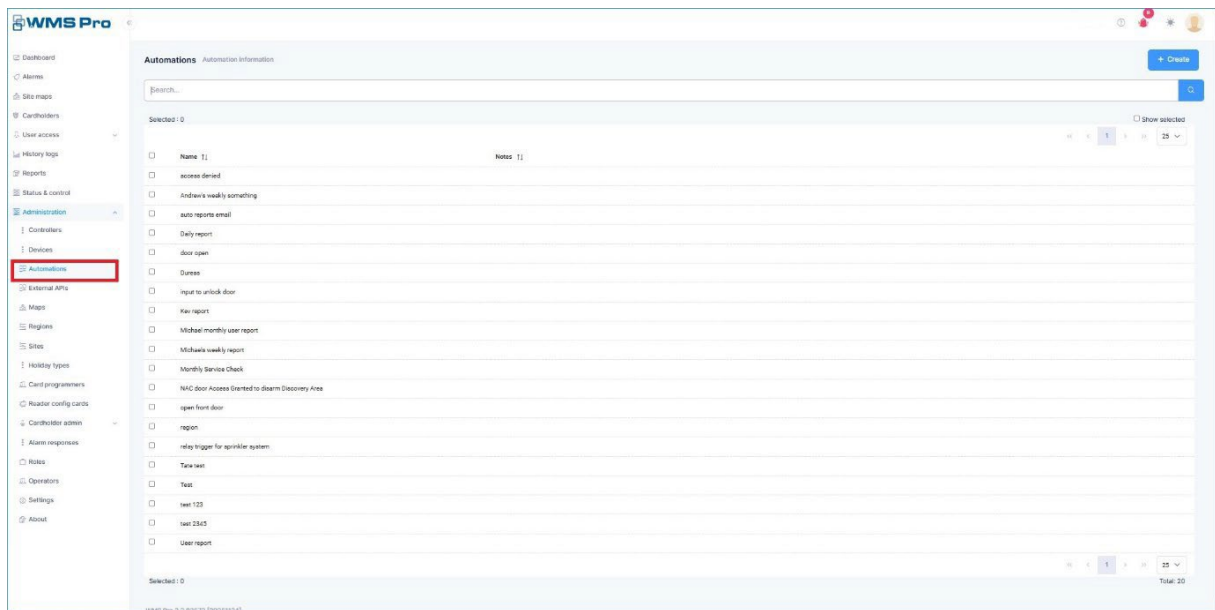
Asset details

Asset details allow you to keep track of your Device's Asset Details. It will allow you to keep track of maintenance, what particulars exist for the asset and even who installed it. Items marked with a '*' are mandatory.

You can generate a [Report](#) to keep track of these Devices asset details.

Automations

Automation information



Enter a search term to narrow down the list to assist with locating a specific automation.

Create automation

To Create an Automation, click the '+ Create' button.

On this page you will need to name your 'Automation', and then use the click drop down arrow to find your 'Region'. You can also add some notes in the 'Notes' section. Check the Enabled box to enable your new 'Automation'. Then click on the 'Save' button.

Once you go back to the 'Automation' list page, if you then click on your 'Automation', you will then come to the 'Edit automation' page. The Automation details is what you just entered to create the automation.

Triggers

The next tab is the 'Triggers' page. You can use the search field to find an event type Trigger. To create a new Trigger, click on the '+ Add trigger' to create one. First you will need to select a **'Trigger type'** of either **'By event'** or **'By schedule'**.

If you click on the **'By event'** Trigger type, you will then have to choose your Event type of either Device, Operator, or Region and the Event type that's relevant from the list.

Trigger Type **'By schedule'** will then give you a 'Repeat type' option for how often this 'Automation' will be carried out. That being: Once, daily, weekly, monthly, weekdays, weekends, or periodic.

Actions

The last tab is the 'Actions' page. Here you can search an 'Action' or click on the '+ Add action' button. To 'Create action' you need to choose an **'Action type'** of either **'Execute command'** or **'Report template'**.

For the **'Execute command'**, choose the Command type of either: Device control, Region control, and Execute Status & Control favourite.

For the **'Device control'** option choose a 'Device' from the drop down and then a 'Command' from a drop down list. **For example:** Choose the 'Device' as 'Foyer PIR' and select the 'Command' as 'Update status'.

In the **'Region control'** option choose the 'Region' from the drop down and the 'Command' from a drop down list.

With the **'Execute Status & Control favourite'** Command type choose the 'Favourite' from the drop down list.

The **'Report template'** option, choose from the drop down 'Report template' then the 'Region filter' and the 'Email to operator' field. Note: Report templates need to be created in the [Reports](#) page first.

Report considerations

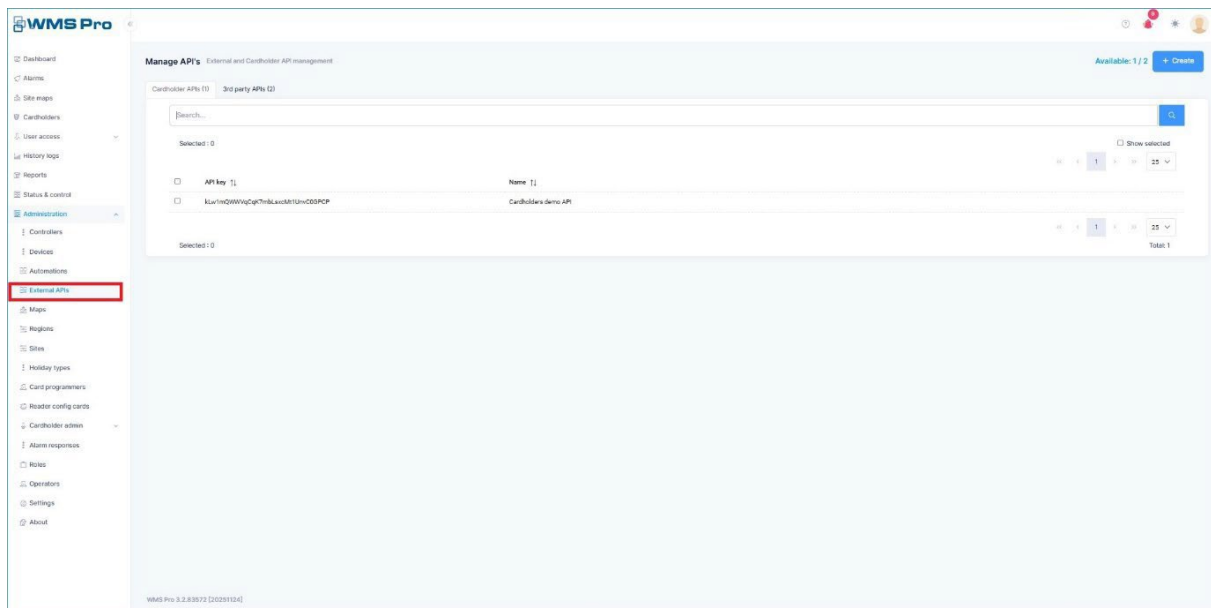
- If an asset tracking report is selected, you will get an additional field called 'Only assets requiring service'. If set to YES, then the resulting report will not include assets with a next service due in the future. If set to NO, then the report will be based on the filters of the report template only.
- If the Operator and Region is not selected, then the logged in Operator's email will be used.
- If no logged in Operator, then there will be no email sent.
- If the Operator is selected, then the email is sent to that Operator, if they have 'Email on event' set.
- If Region is selected, then the email is sent to all Operators that have 'Email on event' set and belong to that Region.
- If Operator and Region is selected, then the email is sent to the selected Operator only.

On the top of the page there are 3 tiles.

1. 'Copy' to copy the automation you have created.
2. '+ Create' to create a new automation.
3. '- Delete' to delete the automation.

External API's

External and Cardholder API management



External API's allow 3rd Party integrations to be implemented by utilising a REST-based API for supported functionality. The Cardholders API can be used to manage Cardholders in WMS Pro from an external system, such as: Active Directory, online booking platforms, visitor management, etc. The 3rd Party API can be used to view and control Devices in WMS Pro, along with their status and event history. All API's are authenticated, bi-directional, responsive, and fully documented.

Search bar

Enter a search term to narrow down the API list to assist with locating a specific Cardholder API or 3rd party API.

APIs can have their details edited by clicking on their name.

They can be deleted by hovering over an API's name and clicking on the  symbol. They can also be deleted in bulk by ticking multiple checkboxes next to the API key and then clicking on the  symbol on the bottom right.

Create/Edit Cardholder API or 3rd Party API

Name

Enter the name of the API.

API key

Press the "Auto generate" button to get a new randomly generated API key.

Region

Pressing the dropdown arrow will display a list of [Regions](#) that can be assigned to the API.

Pressing the  button will open up a pop up window containing a list of Regions that can be assigned to the API. Select one of the Regions and press "OK" to assign it to the API.

Enabled

Tick the checkbox to enable the functionality of the API.

Note: The number of Cardholder APIs or 3rd party APIs that can be created in WMS Pro is tied to the amount approved in the current [License](#) applied.

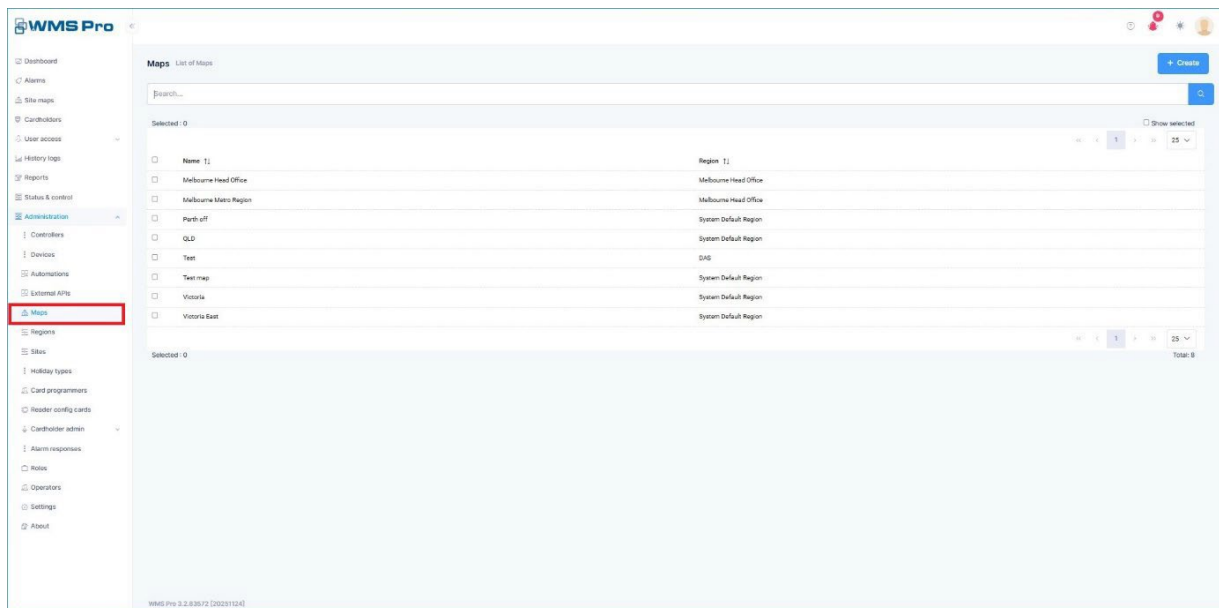
On the top right side of the page, a count is displayed showing how many API licenses are available from the total number the installation is licensed for. This allows Operators to view how many API records may be added before an updated license is required. Please note that this count will reflect the active tab, click on either 'Cardholder API's' or '3rd Party API's' to change tabs and see the available count for the selected API type.

API documentation

The WMS Pro External APIs allow anyone to quickly and easily develop their own integrations with WMS Pro. API documentation for the installed version of WMS Pro can be accessed by clicking [here](#).

Maps

List of Maps



On the 'Maps' page you can 'Search' or choose from a list of 'Maps' that are already created, or you can '+ Create' a new Map.

Create/edit map

First set up a map in WMS Pro, click the 'Create' button and fill in the required fields (explained below). Once the map details have been saved, a new button will appear in the page, '**Design map**'.

Name

Name of the map record.

Region

Assign Map a [Region](#).

This option allows different Maps to exist on the system, whilst only being visible to Operators who have access to the same Region.

Pressing the dropdown arrow will display a list of Regions that can be assigned to the map.

Pressing the  Assign button will open up a pop-up window containing a list of [Regions](#) that can be assigned to the Map. Select one of the Regions and press 'OK' to assign it to the Map.

Design map

This option appears next to the save button once the 'Map' record has been created. Clicking it will load the map designer, allowing you to set a background and place map items. When viewing the map designer, additional options are available to interact with.

<< Back

Pressing this will take you back to the map overview page where the name and Region are specified.

Set background

Allows you to select a map background image file. The background image can be either a JPG, JPEG, or PNG image file with a maximum file size of 5MB. Once selected, a preview of your image will be displayed, allowing it to be resized and cropped as required.

Create map item

Choose type

Select the type of device to be added to the map from the drop down.

- None
- Area
- Automation zone
- Controller
- DGP
- Door
- Floor
- Input
- Lift
- RAS
- Reader
- Map link
- Map text item
- Map image item

Choose icon

Select the type of icon to be used by the selected type (by default this will match the device type you selected). Select icon 'None' if you want to place a rectangle on the screen instead of an image icon. This will appear in the editor as a light blue box to ensure the Operator doesn't lose track of it, however it will appear transparent or displaying the device status colour when viewed on the [Site maps](#) page. The Choose icon options from the drop down consist of the following:

- None
- Area
- Automation zone
- Controller
- DGP
- Door
- Floor
- Input
- Lift
- Ras
- Reader
- Relay
- Custom Icons

Note: Each Icon is physically shown in the Edit window. This makes it easy for an Operator to see if they have the correct Icon.

Note: Custom Icons - These need to be created using svg files, and labelling them: custom01.svg, custom02.svg, ..., etc.

- These svg files need to be put into the: *C:\Program Files\Tecom\WMSPRO\server\wwwroot\assets\common\maps* folder.
- WMS Pro allows up to 99 of these svg files to be created.

Device name

Select the device to assign to the map using either the drop-down selector, or by clicking on the advanced search button to filter and sort available results.

Place item

When 'Place item' is clicked, you'll be taken back to the map, allowing you to click somewhere on the map image to place the item. You can move the icon around the map and resize the item by placing your cursor over the red square on the bottom right of the icon and dragging to resize as desired.

Double clicking on a map item will allow you to edit it, whilst right-clicking on the item will give you the choice to either **Edit map item** or **Remove map item**.

Save

Once all changes have been made, click the Save button to ensure that all changes are saved.

View actual size

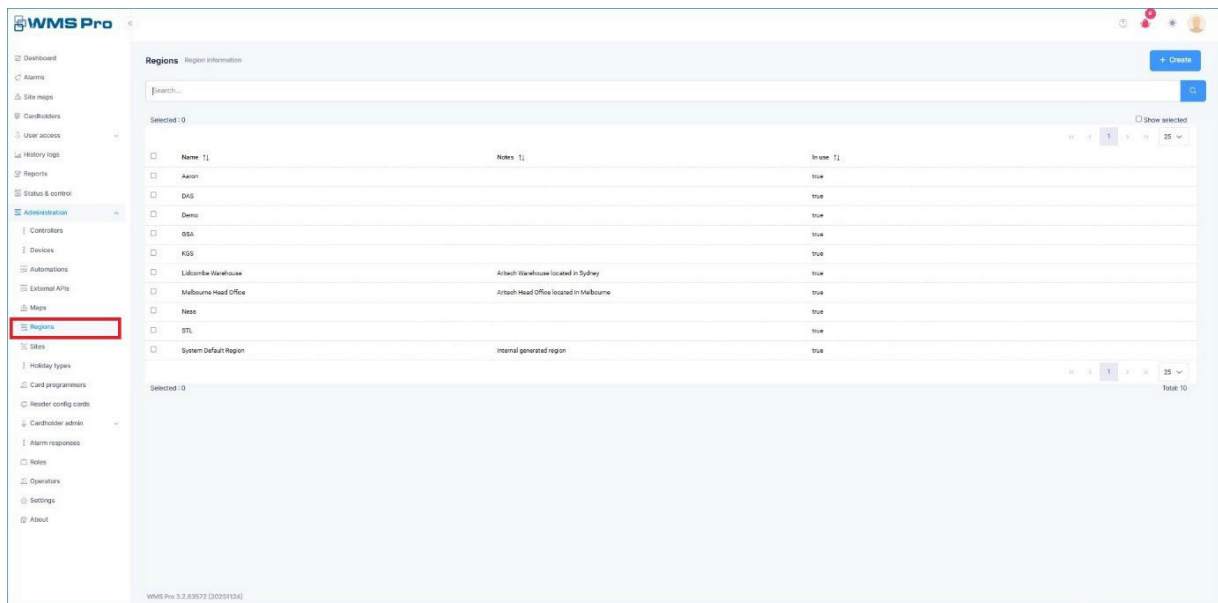
When ticked (default), the map will be displayed at a 1:1 scale for more precise item placement. Unticking this checkbox will adjust the map size to fit within the browser window, providing a more accurate view of what the current map will look like when viewed from the Site maps page.

Remove map item

Will remove the selected item from the map. Alternatively, pressing the 'Delete' key on your keyboard will perform the same action.

Regions

Region information



Regions serve two main purposes:

1. To organise devices and **Cardholders** into groups.
2. To allow **Operators** to view and manage these specific groups.

Regions are not limited to one **Controller**, they can span multiple.

When an Operator is created, they may be assigned to all the Regions or only certain ones. This allows WMS Pro to separate the system so that only certain parts of it are visible to the Operator. This can be useful in multi-tenant situations, or for sites with separated management of staff and devices between distinct business units.

The "In use" column indicates whether a Cardholder, Controller, Device, **Card programmer** etc. is assigned to the Region.

Search bar

Enter a search term to narrow down the Region list to assist with locating a specific Region quickly and easily.

Regions can be edited by clicking on their name.

They can be deleted by hovering over the Region name and clicking on the  symbol. They can also be deleted in bulk by ticking multiple checkboxes next to their name and then clicking on the  symbol on the bottom right.

Create/Edit region

Region Details:

Name

Region name.

Cardholders in region limit

Cardholders in region limit: Click on the Up or Down arrow to increase or decrease the amount of Cardholders allowed in the Region. Having a Region Cardholder limit, e.g., can be used as for a safety measure.

Notes

Optional description an Operator can leave for the Region.

Assigned devices:

Pressing the  Assign button will open up a list of [Devices](#) that can be assigned to the Region. Ticking the checkbox next to the Site name will cause the  icon to appear, press it to unassign the Device from the Region.

This tab is only visible in the edit page of the Region.

Ingress devices:

Pressing the  Assign button will open up a list of [Devices](#) that can be assigned to the Ingress of a Region. Ticking the checkbox next to the Site name will cause the  icon to appear, press it to unassign the Device from the Ingress of a Region.

Egress devices:

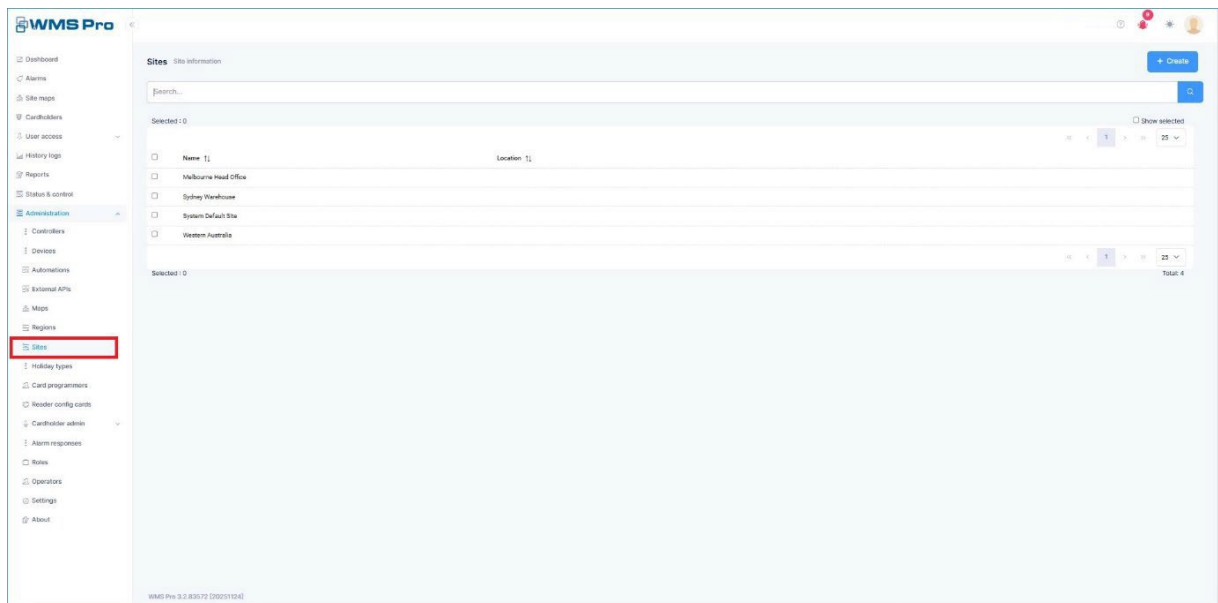
Pressing the  Assign button will open up a list of [Devices](#) that can be assigned to the Egress of a Region. Ticking the checkbox next to the Site name will cause the  icon to appear, press it to unassign the Device from the Egress of a Region.

System Default Region

Cardholders, Controllers and devices by default are assigned to the "System Default Region". They all must always belong to at least one Region, if they have been unassigned from all Regions they will be automatically reassigned to the System Default Region. The maximum assigned Regions can be a total of 10.

Sites

Site information



Sites are used for the organisation of **Controllers**, so that one or more Controller may belong to a Site.

Search bar

Enter a search term to narrow down the Site list to assist with locating a specific Site quickly and easily.

Sites can be edited by clicking on their name.

They can be deleted by hovering over the Site name and clicking on the  symbol. They can also be deleted in bulk by ticking multiple checkboxes next to their name and then clicking on the  symbol on the bottom right.

Create/Edit site

Name

Name of the Site.

Location

Description of the Site location.

Assigned Controllers

Multiple Controllers can be assigned to a single Site; however Controllers can only be assigned to one Site.

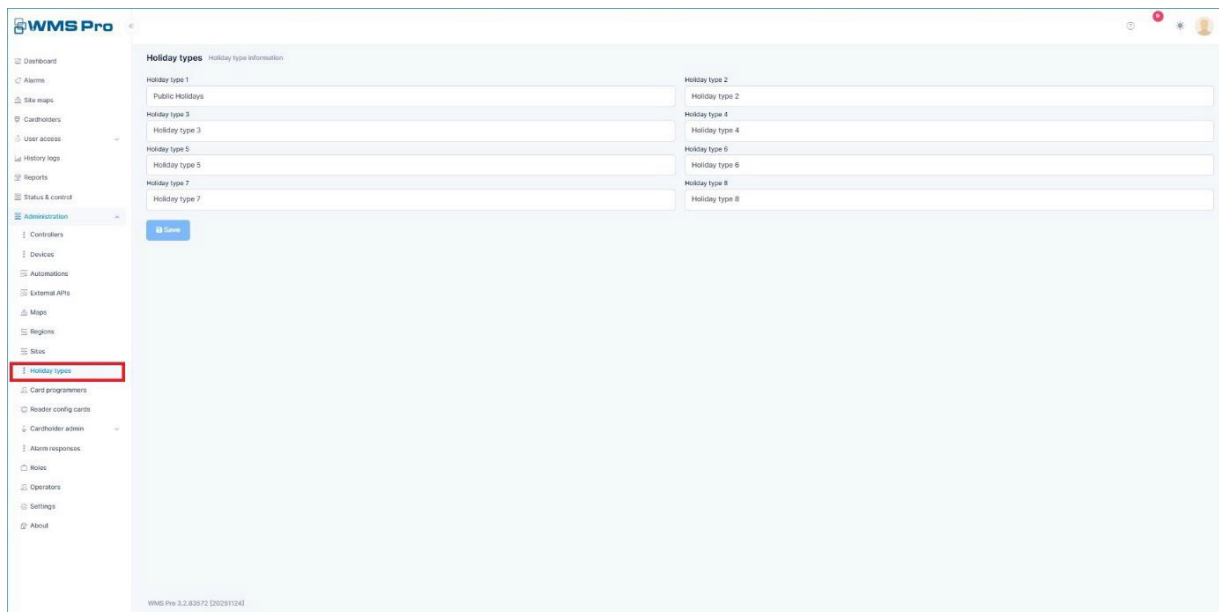
If a Controller has already been assigned to a Site, attempting to assign it to a different Site will result in the previous Site being unassigned.

Pressing the  Assign button will open up a list of Controllers that can be assigned to the Site. Ticking the checkbox next to the Controller name will cause the  icon to appear, press it to unassign the Controller from the Site.

This tab is only visible in the edit page of the Site.

Holiday types

Holiday type information



This page allows the [Operator](#) to **rename** the Holiday types.

Holiday types are used to group Holidays together and provides greater flexibility in controlling access for users during Holidays. If a user's Timezone provides access on Holiday type 1, any Holidays that are not type 1 are excluded (there can be 8 Holiday types).

Holiday types provide the ability to grant access for users on some Holidays and not others. For example:

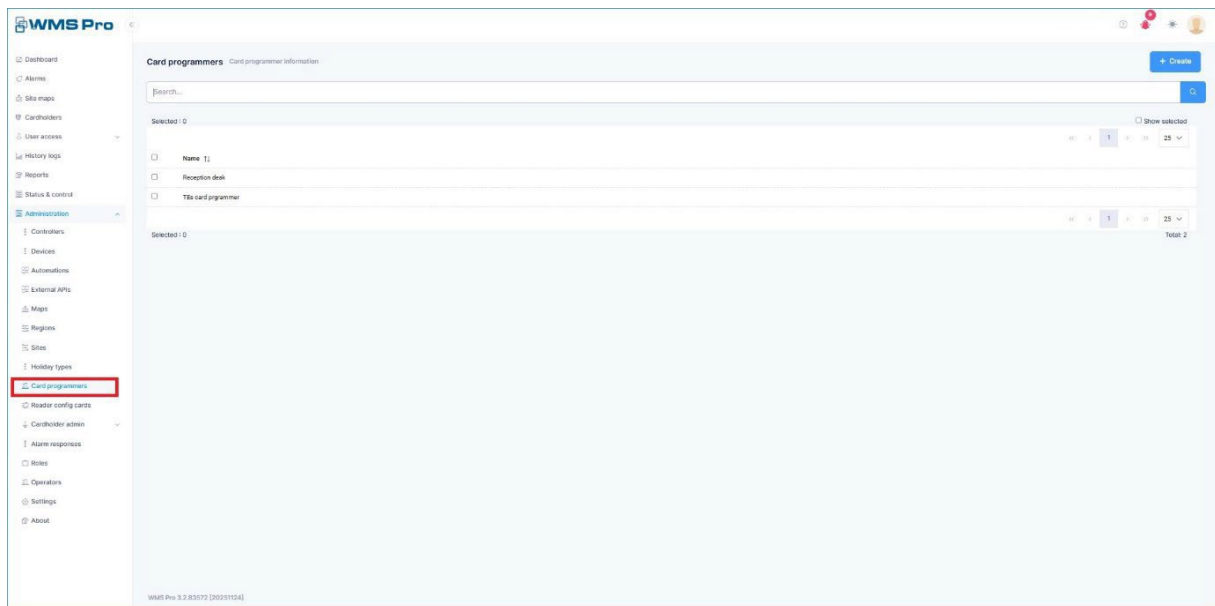
- We want cleaning staff to have access during school holidays, but not on public holidays.
- We want maintenance staff to have access during both school and public holidays.
- School holidays can be designated H1 type, and the cleaning staff Timezone must contain H1 type.
- Public holidays can be designated H2 type, and the maintenance staff Timezone must contain H1 and H2 types.

Holidays can be assigned a Holiday type in the [Holidays](#) menu option.

Timezones can be assigned Holiday types in the [Timezones](#) menu option.

Card programmers

Card programmer information



Card programmers allow an [Operator](#) to program Tecom smart cards (27 bit format cards only) using the Tecom smart Card programmer. A Windows PC is **required** to run the SCPIInterface tool, which is a small program that allows the WMS Pro server to communicate with a programmer connected to the client PC. For more information on SCPIInterface see the **Download installer** section, under the **Edit card programmer** heading below.

Search bar

Enter a search term to narrow down the Card programmer list to assist with locating a specific Card programmer quickly and easily.

They can be deleted by hovering over the Card programmers name and clicking on the  symbol. They can also be deleted in bulk by ticking multiple checkboxes next to their first name and then clicking on the  symbol on the bottom right.

Create/Edit card programmer

Programmer details

To first set up a Card programmer in WMS Pro, click the **"Create"** button and fill in the required fields (explained below). Once the programmer details have been saved, a new button will appear in the page, **"Download installer"**. A new tab will be visible as well, **"Site setup"**.

- **Name** - Name of the Card programmer record.
- **API key** - The API key is used for identification and communication between WMS Pro and the Card programmer, and must be configured in the SCPIInterface tool to match the correct Card programmer record in WMS Pro. Click on the **Auto generate** button to generate a random API key.
- **Connection password** - Allows the Operator to connect to a Card programmer, only required if the Card programmer is programmed to use a password. The password is a 10 digit numerical code, by default it is set to "0000000000".
- **Region** - Assign Card programmer to a [Region](#).

- This option allows different Card programmers to exist on the system, whilst only being visible to Operators who have access to the same Region.
- Pressing the dropdown arrow will display a list of **Regions** that can be assigned to the Card programmer.
- Pressing the  button will open up a pop up window containing a list of Regions that can be assigned to the Card programmer. Select one of the Regions and press "OK" to assign it to the Card programmer.
- **Enabled check box** - Enables communication to the Card programmer.

Download installer

This option appears next to the save button once the Card programmer record has been created. Clicking it will download the **ScpInterfaceInstaller.zip** file, a tool that allows WMS Pro to communicate with the Card programmer. Extract the zip contents to a folder and then run the **ScpInterfaceSetup** application, clicking "**Next**" until the installation has finished.

Scp Interface

Once SCPIInterface has been installed and opened, a new window will appear with the following fields:

COM Port - The COM port refers to the physical port the Card programmer is using to connect to the PC, this field will be required to be manually selected WMS Pro Host - WMS Pro host name API Key - This field will automatically have the API Key that was entered in WMS Pro.

Note: Besides the COM Port, all the other information for the server and connection should be pre-populated to match the Card programmer config page.

Commencing communications

Once the **Start** button has been clicked, the program will initiate communication between the WMS Pro server and the Card programmer. Clicking **Stop** will prevent the WMS Pro server from being able to communicate with the Card programmer until it is started again.

Site setup

This tab will only appear once the Card programmer record has been created.

- **Card security password** - Type a security password (also known as the 4-byte code) in the range of 0 to 127 in each field. The smart Card programmer stores the password and writes the number to the cards. Cards can only be erased or blanked if the Card programmer's security password matches the one found on the card. This number must also match the security password stored in the smart card reader for the cards to work.
- **Card password lock** - If this check box is *Ticked*, cards programmed with the programmer cannot be blanked/erased or changed to Reader Configuration Cards. The cards may only be programmed to different users of the same 4-byte Card security password.
- **+ Add site code range** - Provides the Operator the ability to add a defined range for the site code. Can have multiple site code ranges. Enter numbers in the minimum and maximum fields to establish the range. Press the  button to remove the site code range.
- **Retrieve settings** - Retrieve the settings already found in the Card programmer and overwrite the current settings found in Site setup.

Reader Configuration cards

Configuration card information

The screenshot shows the WMS Pro interface for configuring a reader. The left sidebar contains a navigation menu with items like Dashboard, Alarms, Site maps, Cardholders, User access, History logs, Reports, Status & control, Administration, Controllers, Devices, Automations, External APIs, Maps, Regions, Sites, Holiday types, Card programmers, Reader config cards (highlighted with a red box), Cardholder admin, Alarm responses, Roles, Operators, Settings, and About. The main content area is titled 'Configuration card' and 'Configuration card information'. It features several dropdown menus and checkboxes for configuring the reader's behavior, such as 'Reader address' (set to 1), 'Reader options' (Door output, Security mode, Online/LED options), 'Protocol options' (Wiegand), 'Egress controls' (Egress disabled), 'Offline LED options' (Door open only, Two wire operation), and checkboxes for 'Valid card beep', 'Valid card LED flash', and 'Read option card'. A 'Write default config card' button is located in the top right corner.

This page is used to set up a configuration card.

Configuration card information

Reader address

Enter a value in the range 1 to 16 if the reader is configured as a LAN device. If the reader is connected to a Door Controller sub-LAN, the address determines the Door it controls and direction it travels.

Protocol options

This field determines the protocol that the reader will output to the Controller. For non mag-swipe readers, leave the protocol set to *Wiegand*.

Reader options

Door output - The output follows the Door lock output time. The relay output (violet wire) will operate as a Door relay control output (active low) when 'online' only.

Tamper output - The reader contains a built in tamper. This output follows the tamper status.

Card present output - The relay output will activate when a magnetic stripe card (smart card) is presented (active low) to a Track 2 magnetic stripe interface, when in the 'offline' mode only.

Card output timed - The relay output operates as a timed output if the reader is set up as a credit activated device. The relay output will be activated when a credit transaction is successfully completed.

Card output pulsed - The relay output operates as a pulsed output (active low) set up as a credit activated device.

Card output latched - The relay output will operate as a latched output if the reader is set up as a credit activated device. When a Tecom smart card with valid credit data is badged, and the transaction is successfully completed, the relay output is turned on. The relay output is turned off when a valid Tecom smart card is next badged.

Egress controls

Egress disabled - The egress function on the reader is disabled.

Egress only - Operates with the TS0064 push button or any single poll push button connected to the egress input on the RJ45 connector.

Egress and arm disarm - Requires the TS0064 push buttons. Any single poll push button may be connected to the egress input of the TS0064 for egress operation.

Security mode

Secured mode - the reader will see programmed Tecom smart cards with credit facilities and user defined cards.

Unsecured mode - the reader will only see blank (unprogrammed) cards with a unique serial number and user defined cards.

Note: In *Unsecured mode*, both the Challenger panel and any Intelligent Door/Lift Controllers must use IUM (Intelligent User Memory) so that the Challenger can learn the card data.

Online blue LED options

The reader is said to be *online* when it is configured as a LAN device either on the Challenger LAN or the Intelligent Door/Lift Controller sub-LAN.

The two options are:

Door open only - the blue LED will normally be off and flash whilst the Door lock relay is active, and

Access and door open - the blue LED is ON when the alarm area associated with the Door is in access and flash whilst the Door lock relay is active.

Online red LED options

Secure - the red LED is ON when the area associated with the Door is secure.

Secure and door open - the red LED is ON when the area associated with the Door is secure and flashes whilst the Door lock relay is active.

Offline LED options

The reader is considered to be in *offline* mode when it is configured as a Wiegand device.

In this mode there are two options for LED operation:

Two wire operation - enables the operation of the red and blue LEDs via their respective two wires. The brown wire, when grounded, activates the red LED and the yellow wire, when grounded, activates the blue LED.

One wire operation - the brown wire controls both LEDs. When grounded, the blue LED is lit and when +5 to +12 VDC is applied, the red LED illuminates.

Valid card beep

When *Ticked*, the reader sounder will beep when a valid card is presented.

Valid card LED flash

If *Ticked*, the blue LED will give one flash when a valid card is presented.

Watchdog

Can only be used if the reader is configured as a Wiegand device. The watchdog checks the reader's CPU to ensure continuous operation.

Read option card

If this box is *Unticked*, the reader can only be configured with a Reader Configuration Card once. Any future changes must be made via the Challenger RAS (keypad) or by first unflagging this option via the Challenger RAS (keypad).

Write

Clicking the **Write** button causes the smart Card programmer to write the information to the card.

Blank

The **Blank** button clears the card of all information.

Write default config card

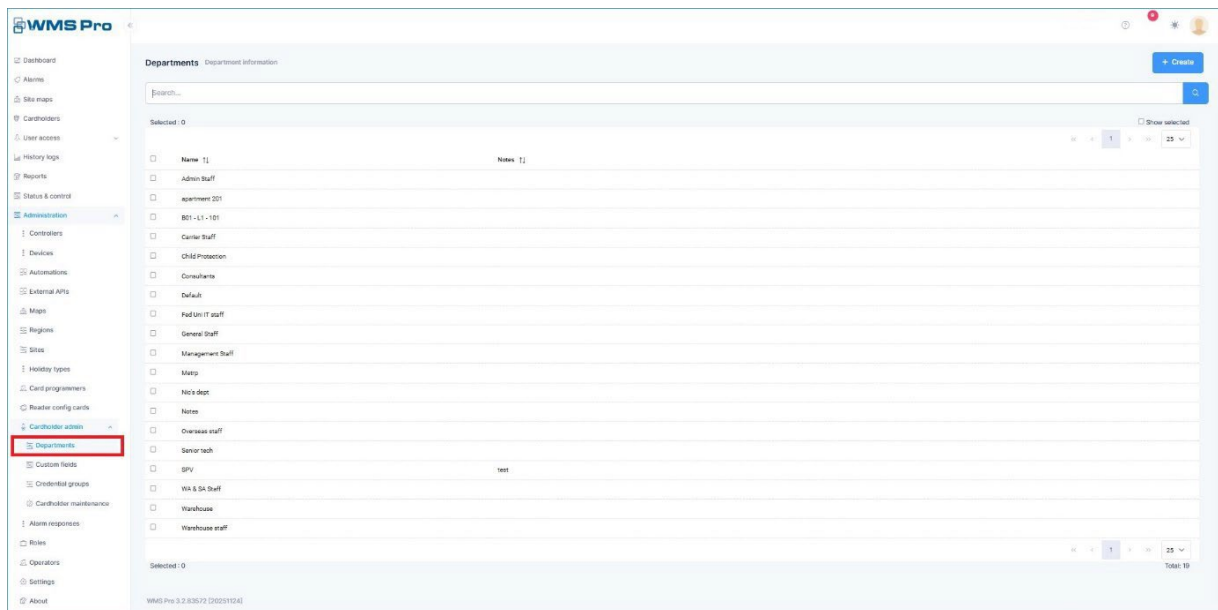
This action is found at the top right of the page. Choose a Card programmer to be connected. Card programmer record must first be created in the [Card programmers](#) menu option.

Note:

The **Write**, **Blank** and **Write default config** buttons will not appear for the Operator if the permissions were not approved for them. In the permission drop down list, the relevant authorisations can be found under **Card programmer controls**. Visit the [Operators](#) page to modify individual Operator permissions, or go to the [Roles](#) page and modify the permissions based on the Operator's assigned Role.

Departments

Department information



Departments can be assigned to [Cardholders](#) as a way to categorise them. Departments also give Cardholders access to [Custom fields](#) attached to the Department.

Search bar

Enter a search term to narrow down the Department list to assist with locating a specific Department quickly and easily.

Clicking on any of the Department names in the list will open up the edit page for that Department.

Departments can be deleted by hovering over a Department's name and clicking on the  symbol. They can also be deleted in bulk by ticking multiple checkboxes next to their name and then clicking on the  symbol on the bottom right.

Create/Edit Department - Department details

Name

Name of the Department.

Notes

Optional field to provide details of the Department. The notes window can be resized by hovering over the bottom right side of the window and clicking and dragging the corner.

Design card

+ Create card item

Choose the item type to add to the Photo ID card from the drop down list:

- Label
- Last name
- First name
- Department
- Email
- Employee ID

- Cardholder image
- Static image
- Custom field property 1
 - Choose field e.g, Vehicle registration
- Custom field property 2
 - Choose field e.g, Registration expiry

Each item will have different properties to be populated. E.g, Alignment & transparency, fonts, options for Bold and Italic text, colour of card ...etc.

Portrait / Landscape

Option to choose the card's layout of either 'Portrait' or 'Landscape'.

Front side / Back side

Build card items on the Front side and Back side of the card.

Items

This button allows a list of what has been created on the card's side of choice. Click on each 'Card item' to see where it is on the card.

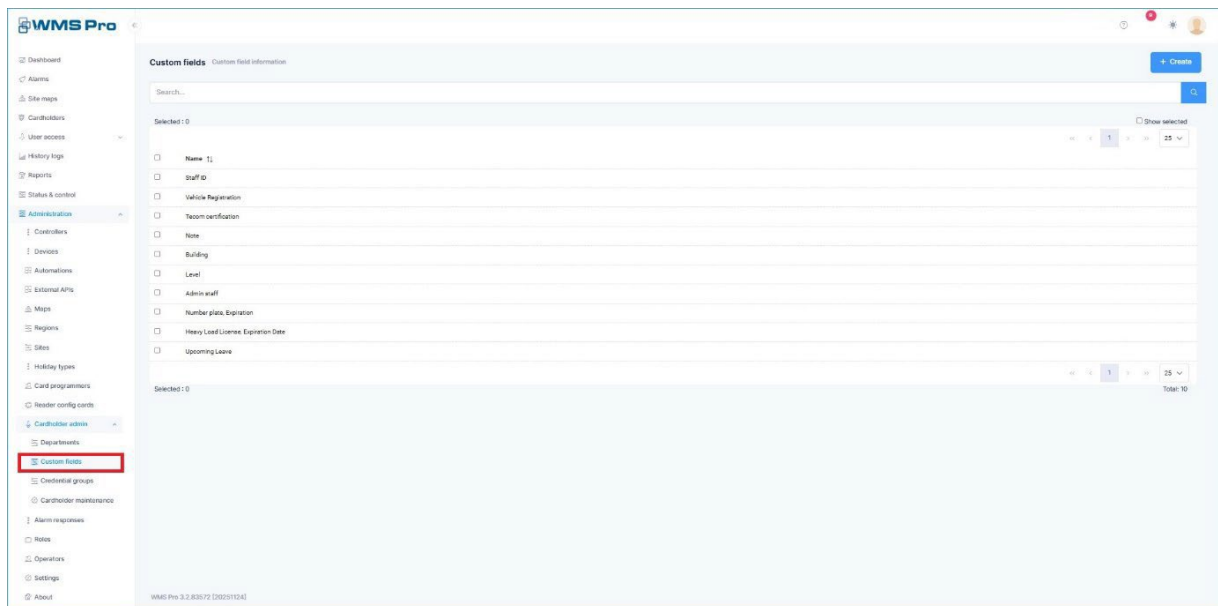
- **Remove card item** or **Remove all** option to delete information added to the card.

Assigned custom fields

This tab lists out [Custom fields](#) that have been assigned to the Department. Pressing the  Assign button will open up a list of Custom fields that can be assigned to the Department. Ticking the checkbox next to the Custom field name will cause the  icon to appear, press it to unassign the selected Custom fields from the Department.

Custom fields

Custom field information



Custom fields provide a way for [Cardholders](#) to have role specific information tied to their profile, for example: a Custom field that is used to accept license numbers for forklift drivers. A newly created Custom field will appear in the **User details** tab of the Cardholder's create/edit page as an empty field. These fields are linked to the [Departments](#) they are created in and will only appear for Cardholders assigned to said Department.

Search bar

Enter a search term to narrow down the Custom fields list to assist with locating a specific Custom field.

Custom fields can have their details edited by clicking on their name.

They can be deleted by hovering over a Custom field's name and clicking on the  symbol. They can also be deleted in bulk by ticking multiple checkboxes next to their first name and then clicking on the  symbol on the bottom right.

Create/Edit Custom fields

In this page select the field **Type** and enter the name of the custom field in the **Display text/Display text for date** to create it.

Type:

- Text - Accepts alphanumeric and special characters. Enter display text to name the field.
- Number - Only accepts numeric characters. Enter display text to name the field.
- Date only - Only accepts a date as an input. Enter display text to name the date field.
- License - This option has two fields, one for alphanumeric and special characters, and one for a single date. Enter display text to name the license and date field.
- Date range - Accepts two dates that define a date range. Enter display text to name the date range field.

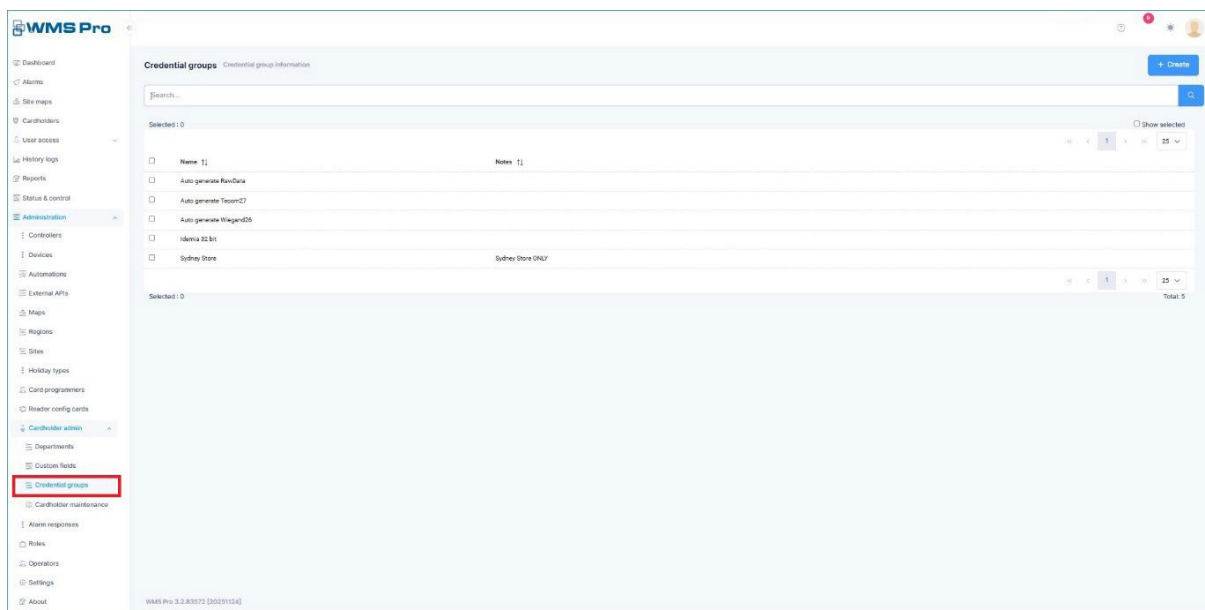
Assigned departments

Use the 'Search' bar to filter the list of assigned departments.

'Assign' button (either top or bottom) will open a popup window that contains a list of departments that are not already assigned to this custom field. Select any of the departments within popup window and press 'Ok' to assign to this custom field.

Credential groups

Credential group information



Credential groups are what help WMS Pro determine which Cardholder belongs to which Controller. As long as they both share the same Credential group, then the Cardholder's details will be sent to that Controller.

Search bar

Enter a search term to narrow down the Credential group list to assist with locating a specific group. You can filter by columns except for the card number column.

Credential groups can be edited by clicking on their name.

They can be deleted by hovering over their name and clicking on the  symbol. They can also be deleted in bulk by ticking multiple checkboxes next to their name and then clicking on the  symbol on the bottom right.

Create/Edit credential group

Name

Credential group name.

Card Format

Choose the card format type from the drop down menu.

Create/Edit custom Card format

To create your own custom card format click the + icon next to the Card format drop down arrow.

Add new custom card format details:

- Format name: specify the name of your custom card format
- Total bit length: this value should be automatically generated from the sum of:
 - Site code length
 - Card number length

- Number of parity types in use (i.e parities set to 'Even or Odd')
- Site code start bit / length: specify the first bit and the number of bits used by the site code.
- Card number start bit / length: specify the first bit and the number of bits used by the card number.
- 3 x parity settings (P1, P2, P3), consisting of:
 - Type:
 - None (default): parity will not be used. If the custom card format requires less than 3 parity calculations, the unused parities should be set to this.
 - Even: the parity bit will be set to either 1 or 0 to ensure that the total number of '1' bits in the defined parity locations is even.
 - Odd: the parity bit will be set to either 1 or 0 to ensure the total number of '1' bits in the defined parity locations is odd.
 - Parity bit: specify which bit number will be updated based on parity calculations.
 - Parity bit start / length: specify the first bit and number of bits used by the parity calculations.
- 'Save' button: creates the format and returns the Operator to the create/edit Credential group page.
- 'Cancel' button: cancels any unsaved changes and returns the Operator to the create/edit Credential group page.

Note: Selecting "Tecom 27 bit" will allow the [Cardholder](#) to program their Credentials into a Tecom smart card. See [Card programmers](#) for more information.

Default site code

Input the site code. This is an optional field, if a code is entered in then it will prefill the site code for the Cardholder if the Credential group is chosen.

Notes

Add any other additional notes for the Credential group.

Once the Credential group details have been Saved you will then see a 'Assigned credential' tab appear.

Assigned credentials

This allows Operators to see which credentials are assigned. Credentials can be edited from this page by clicking on the blue person icon at the end of the row. This will then open up a box called 'Edit Credential(s)'.

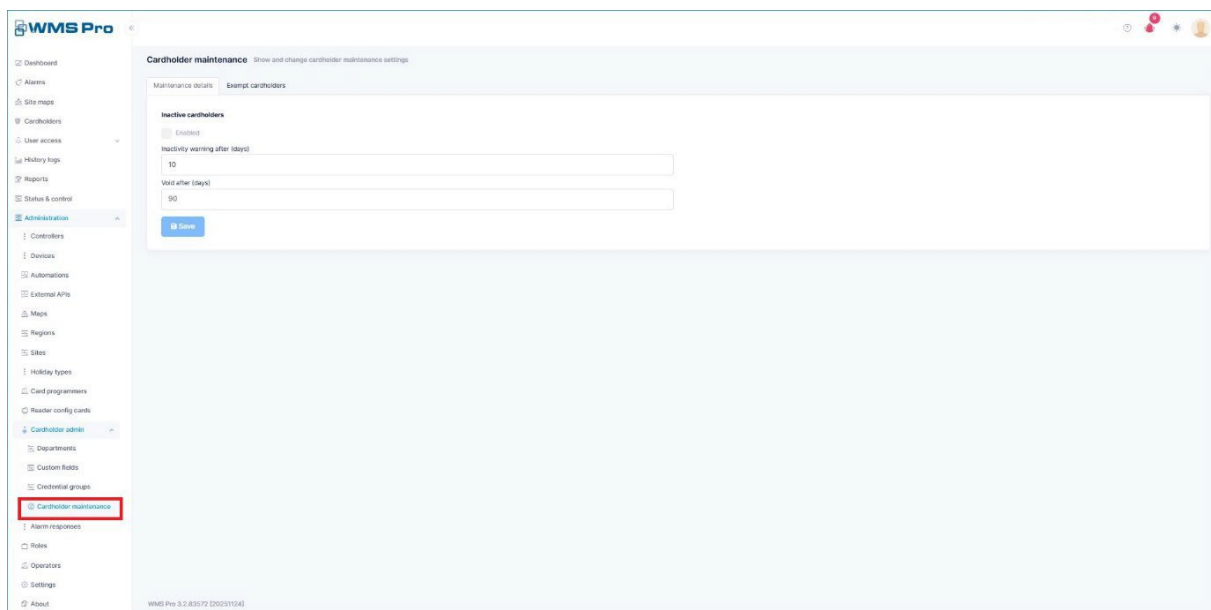
From here you can edit credentials e.g. change status, start date, user flags ...etc.

You can delete credentials from this tab which will remove credentials and unassign from the cardholder. Cardholder will be deleted from panel.

The Operator has to have Credential groups, view cardholders, edit cardholders, delete cardholders permissions to be able to edit these fields.

Card maintenance

Show and change cardholder maintenance settings

The screenshot shows the 'Cardholder maintenance' page in the WMS Pro application. The page has a sidebar on the left with a navigation menu. The main content area is titled 'Cardholder maintenance' and contains two tabs: 'Maintenance details' (selected) and 'Exempt cardholders'. Under the 'Maintenance details' tab, there is a section for 'Inactive cardholders'. This section includes a checkbox for 'Enabled', which is currently unchecked. Below the checkbox are two input fields: 'Inactivity warning after (days)' with the value '10' and 'Void after (days)' with the value '90'. A blue 'Save' button is located at the bottom of this section. The sidebar on the left lists various system components, with 'Cardholder maintenance' highlighted in red. The bottom of the page shows the version 'WMS Pro 3.2.830/72 (20231104)'.

Maintenance details

With the 'Cardholder maintenance' page you can select how many days a Cardholder can be inactive before they will receive an 'Inactivity warning'.

Also, you can select how many days after the Inactivity warning the Cardholder's card will become void. This has to be more than the Inactivity warning or you will receive an error warning.

Then click the 'Enabled' button and the 'Save all' button to activate these warning times.

In an example if we had an 'Inactivity warning after' 30 days and the card became 'Void after' 60 days. The cardholder's card would have 30 days to the warning and then another 30 days till it becomes Void.

You can generate an 'Inactive cardholder report' via the Reports page in WMS Pro.

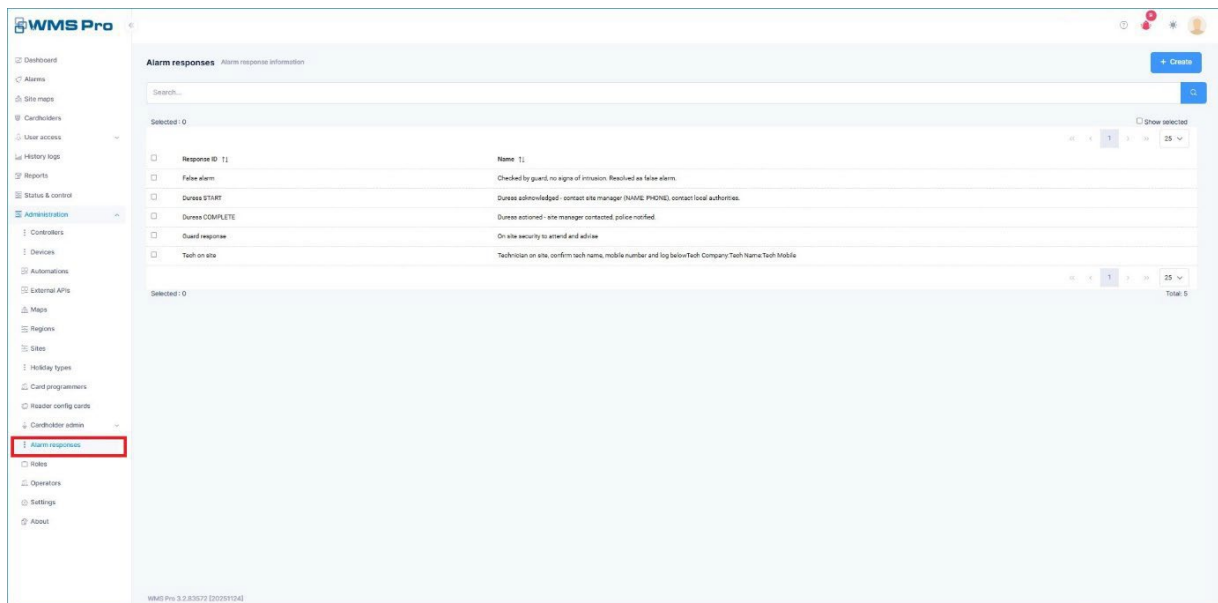
Exempt cardholders

Click the + Assign button to see a list of Cardholders. Tick the checkbox next to the Cardholder(s) name(s) and click OK to save the Cardholder(s) to be exempt from getting the warnings.

On the list of exempt Cardholders, tick the checkbox next to the Cardholder(s) name, and click the blue minus button to unassign the Cardholder(s) from the exempt Cardholder list.

Alarm responses

Alarm response information



This page lets the operator create custom preset **Alarm** responses to be used when entering a response to an active Alarm.

Search bar

Enter a search term to narrow down the response list to assist with locating a specific response.

Alarm responses can have their details edited by clicking on their name.

They can be deleted by hovering over an Alarm response's name and clicking on the  symbol. They can also be deleted in bulk by ticking multiple checkboxes next to the Response ID and then clicking on the  symbol on the bottom right.

Create/Edit Alarm response

Response ID

Enter the name of the response type.

Response text

Enter the description of the response.

Region

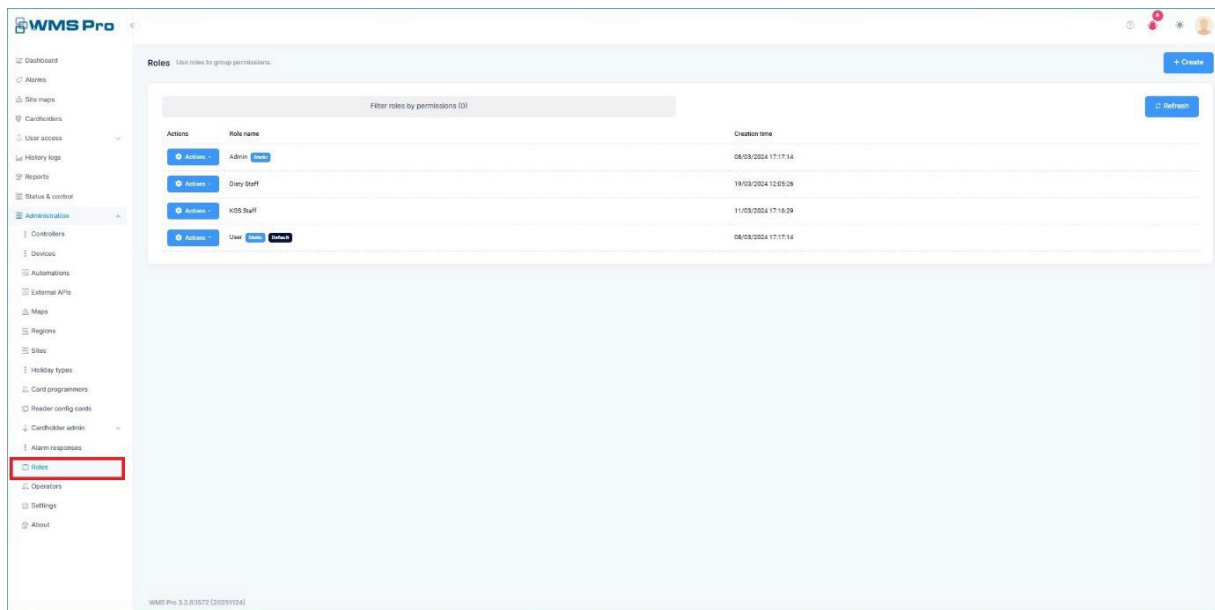
Click the Region drop down to select your Region.

Assigning an Alarm response to a region allows multiple similar responses to be used across the WMS Pro system, whilst ensuring that specific responses are only visible to appropriate Operators.

For Example: A Duress Alarm might have different requirements and contact information depending on the location. By assigning the correct Region to each response, you can have a Duress response for 'Region A' and a different Duress response for 'Region B'. Without having to worry about Operators in each location accidentally selecting the wrong response. Likewise, this can be used to prevent a lower-level Operator from accessing advanced responses intended for higher-level Operators with specific situational training.

Roles

Use roles to group permissions



Roles determine what permissions the Operators in WMS Pro have. New Roles can be created with certain authorisations allowed specifically for the Role.

Filter Roles by permissions

This functionality allows the Operator to find Roles based on what permissions have been approved for said Role.

Create/Edit role

Role Name

Name of the Role.

Default

Tick this checkbox to have the Role automatically assigned to new Operators.

Permissions

Role permissions can be determined by ticking the check boxes for the relevant actions. When an Operator is allocated a Role, they are automatically given the same permissions approved under that Role. However, the Operator's permissions can still be configured in the [Operators](#) page and doing so will modify the permissions for that Operator only.

Some permissions have subset permissions underneath them. For example, the **"Controllers"** permission is the adult, and **"Create new controller"** is a child permission. Ticking the adult permission will automatically tick all the child permissions underneath it. Ticking the child permissions will automatically tick all the adult permissions above it.

Read only permissions

To enable read only permissions for a Role, tick the checkbox for the adult permission but leave the child ones unticked. For example, to provide read only permission for **Controllers** tick the checkbox for "Controllers" but untick "Create new controller", "Create new device" and the rest of the child permissions. As a result the Role will allow the Operator to view the Controllers, but they will have no options to change any of the settings.

Actions

Edit

Edit the details of the Role. See the section "Create/Edit role" above for more information.

Delete

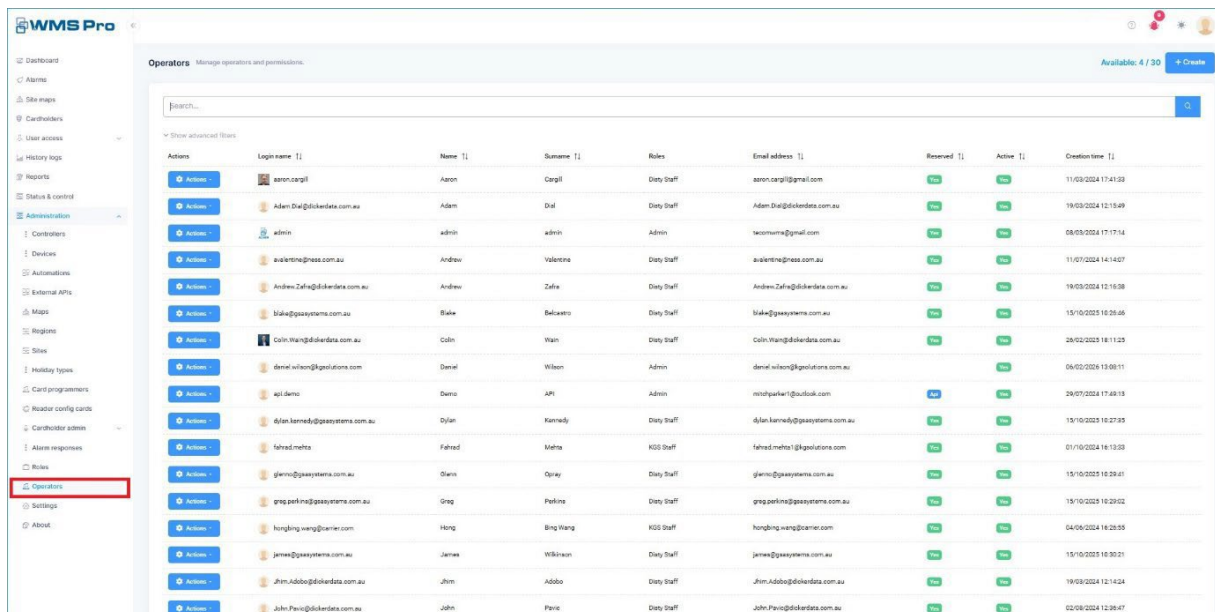
Remove the Role from WMS Pro. This option only appears for Roles that do not contain the  tag next to the Role name.

Assigning Roles

Roles can be assigned to Operators in the [Operators](#) page, however the Operator currently logged in and making the changes can only assign Roles that they have access to.

Operators

Manage operators and permissions



Actions	Login name [1]	Name [1]	Surname [1]	Roles	Email address [1]	Reserved [1]	Active [1]	Creation time [1]
Actions	aaron.cargill	Aaron	Cargill	Dirty Staff	aaron.cargill@gmail.com	☒	☒	11/03/2024 17:41:33
Actions	Adrian.Dal@gliderdata.com.au	Adrian	Dal	Dirty Staff	Adrian.Dal@gliderdata.com.au	☒	☒	19/03/2024 12:15:49
Actions	admin	admin	admin	Admin	twomurmes@gmail.com	☒	☒	08/05/2024 17:17:14
Actions	avalemtne@pess.com.au	Andrew	Valentine	Dirty Staff	avalemtne@pess.com.au	☒	☒	11/07/2024 14:14:07
Actions	Andrew.Zahag@gliderdata.com.au	Andrew	Zahag	Dirty Staff	Andrew.Zahag@gliderdata.com.au	☒	☒	19/03/2024 12:16:38
Actions	Blake@pessystems.com.au	Blake	Belavero	Dirty Staff	Blake@pessystems.com.au	☒	☒	15/10/2023 16:29:46
Actions	Colin.Wang@gliderdata.com.au	Colin	Wang	Dirty Staff	Colin.Wang@gliderdata.com.au	☒	☒	28/02/2023 18:11:25
Actions	daniel.wilson@gliderdata.com	Daniel	Wilson	Admin	daniel.wilson@gliderdata.com	☒	☒	06/02/2023 13:08:11
Actions	dapi.demo	Demo	API	Admin	michigawell@outlook.com	☒	☒	29/07/2024 17:49:13
Actions	dylan.kennedy@pessystems.com.au	Dylan	Kennedy	Dirty Staff	dylan.kennedy@pessystems.com.au	☒	☒	15/10/2023 16:27:35
Actions	felixad.melita	Felixad	Melita	KGS Staff	felixad.melita@gliderdata.com	☒	☒	01/10/2024 16:13:33
Actions	glenn@pessystems.com.au	Glenn	Olney	Dirty Staff	glenn@pessystems.com.au	☒	☒	15/10/2023 16:29:41
Actions	greg.perkins@pessystems.com.au	Greg	Perkins	Dirty Staff	greg.perkins@pessystems.com.au	☒	☒	15/10/2023 16:29:02
Actions	hongling.wang@carrier.com	Hong	ling Wang	KGS Staff	hongling.wang@carrier.com	☒	☒	04/06/2024 16:29:35
Actions	james@pessystems.com.au	James	Wilkinson	Dirty Staff	james@pessystems.com.au	☒	☒	15/10/2023 16:30:21
Actions	jhm.adobe@gliderdata.com.au	Jhm	Adobe	Dirty Staff	jhm.adobe@gliderdata.com.au	☒	☒	19/03/2024 12:14:24
Actions	John.Pewis@gliderdata.com.au	John	Pewis	Dirty Staff	John.Pewis@gliderdata.com.au	☒	☒	02/08/2024 12:06:47

This page has a list of all visible Operators in WMS Pro. Operators accessing this page can only see other Operator accounts that have an **equal or lesser** Role than them. Operator's permissions and Roles can be configured on this page, either to limit or expand the level of access they have on WMS Pro. Operators can also be allocated to existing Regions.

On the top right side of the page, a count is displayed showing how many Operator licenses are available from the total number the installation is licensed for. This allows Operators to view how many other Operator records may be added before an updated license is required.

Search bar

Specific Operators can be found by typing in a search term to narrow down the results list.

Under the **Advanced filters** option: Operator **Roles**, **Permissions**, and **Only locked Operators** can be filtered based on the selection. Click the refresh button to update the search results.

Advanced filters now remember the state of the filter list after closing the page (only for: **Roles**, and **Only Locked Operators**). On return to this page, these filters will be the same from earlier.

By clicking on the **"Only locked Operators"** slider it will limit the search results to those that have been locked out.

Create/Edit operator

Operator information

Operator user information can be configured in this tab. This includes first and last name, email address, phone number, login name, and password.

The Operator's profile picture can also be changed; their picture can be uploaded by clicking on the **"Change profile picture"** button and selecting the relevant image.

- **Should change password on next login** - The next time the Operator logs in they will be prompted to change their password. This option will be automatically unselected after the Operator logs in and changes their password in the prompt.

- **Send activation email** - The checkbox will be unelectable until the SMTP [Settings](#) have been provided.
- **Active** - Active account.
- **Two factor authentication enabled** - Tick this option to enable 2FA logins for this Operator. Please note that this option can only be enabled when 'Enable two factor operator login' is ticked on the [Settings](#) page and the browser has been refreshed.
- **Lockout enabled** - Lockout settings such as number of failed login attempts allowed and lockout duration can be configured in the Settings page. After exceeding the maximum amounts of failed login attempts the Operator will be locked out for a set duration of time and a  icon will appear next to their login name.
- **External API operator** - Tick this option to give the Operator the API flag necessary for the [API](#) functionality. It should be noted, Operators with this tag will not be able to log in to WMS Pro.
- **Email on event** - Tick this option to make the system email the Operator once an Event has occurred. This will be good for record keeping.
- **Disable override alarm** - Tick this option to allow the Operator to be able to disable override alarms.
- **Use reserved seat** - To be able to use a Reserved seat the checkbox has to be checked in the Operator information page.

Note: Reserved Seating

The Reserved Seating for the Operators works like for example: If you have 3 licenses and 2 are set as Reserved and you have 4 Operators. The 2 non-reserved Operators cannot both login because it has to always keep 2 spots open for the Reserved Operators. So in this example, you only have 1 floating license. So only 1 non-reserved Operator at a time.

When an Operator has been allocated a Reserved Seat a Green Yes tag will be against their name. Also when an Operator is 'Active' they will also have a Green Yes tag against their name.

Note: External API Operator

When an Operator is an External API Operator, there will be a blue API tag against their name. Also 'External API Operator' are not included in the Operator license count.

Roles

Tick the check box to assign [Roles](#) for the Operator. Depending on the Role assigned, the Operator will have role-specific permissions granted to them. When selecting multiple roles, all the permissions for each of the roles will be merged and assigned to the Operator.

Note: When assigning Roles to another Operator, only Roles equal to or lesser than (in regard to Role permissions) the Operator currently logged in can be selected.

Region permission

Operators can be assigned to [Regions](#) that appear in the list. By ticking the "Full region permission" checkbox the Operator will be given full permission for all existing and future Regions.

 Actions

Edit

See the "Create new Operator/Edit Operator" section above.

Permissions

Operator permissions can be edited under this option page. Permissions will be automatically populated based on what Role was assigned, however these permissions can still be customised for the Operator. If you want to reset the customised permissions and revert them to the default Role permissions, click on the "**Reset special permissions**" button on the bottom of the pop up window.

Note: An Operator cannot assign permissions to another Operator that they themselves do not have.

Permissions for Operator connecting to WMS Pro via CTPlus

To ensure that Operators connected to WMS Pro through CTPlus face no errors, the following permissions should be granted: **Card programmers** (and all the child permissions under it), **Controllers** (and all the child permissions under it), **Dashboard**, and **Status & control** (and all the child permissions under it).

Unlock

If an Operator gets locked out from the system due to multiple failed login attempts a  will appear next to their login name. Clicking the "unlock" option will undo the lockout, remove the padlock icon, and allow the Operator to login again.

This option will be visible only for Operators that have been locked out.

Notes on removing the icon for an Operator

There are two ways to have the padlock symbol be removed for the Operator; they are "**Unlocked**" in the **Actions** command, or the lockout timer has expired. (Lockout time remaining is shown) After the lockout duration has timed out the padlock will be removed.

Delete

Removes the Operator from the WMS Pro system.

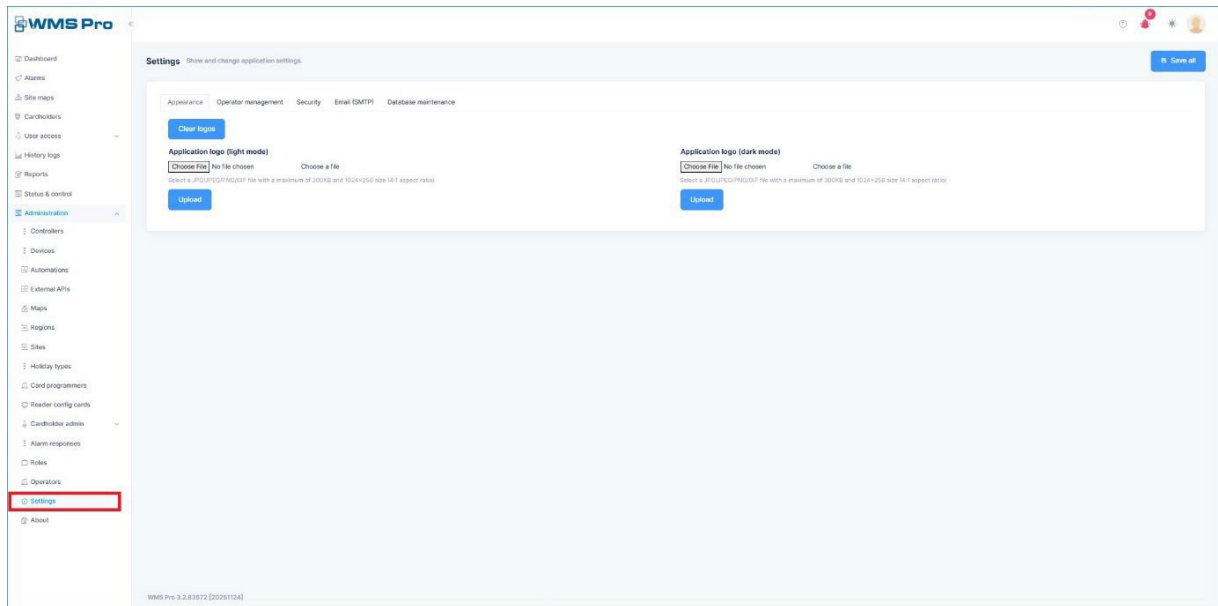
Force logout

This is available to force an Operator to logout if you need to adjust the Reserved Seating for availability of Operators.

Note: For an Operator to be able to use the Action option or the sub actions under it (edit, permissions, delete and unlock), ensure the "Changing permissions" option is approved in the Operator's permissions.

Settings

Show and change application settings



Miscellaneous WMS Pro settings such as the logo and password requirements can be configured on this page.

Appearance

The application logo on the top left of the screen can be replaced with a logo of the Operator's choosing. Click "**Choose File**" to browse for the image. Once the desired image has been selected, click the "**Upload**" button to finalise the changes. Click "**Clear logos**" to return to the default logo.

There is an option to customise the application logo for light mode and dark mode separately, it should be noted however that customising the logo for dark mode exclusively will make it the default logo for both light and dark mode.

Note: Any changes to the application logo will also be applied to the logo in the login screen. The dark mode logo will take priority over the light mode logo if both have been customised.

Operator management

Session Timeout Control

When no activity during the session of WMS Pro has occurred, the session **will** timeout after a set period. The 'Session Time Out Control Enabled' is always ticked, greyed out and locked.

After a session timeout, a WMS Pro locked screen will show, if the 'Show Lock Screen When Timed Out' is enabled.

Timeout (seconds)

This is the time out for inactivity of the WMS Pro site. It will lock the Operators screen after a set time. The Default is set to 1200 seconds (20 minutes). Minimum can be set to 300 sec (5 Minutes) and Maximum can be set to 1800 sec (30 minutes).

Countdown Modal Wait Time (Seconds)

When Session Timeout is reaching the end of its period, a blue countdown timer bar will be displayed counting down to the end of the Session. This timer can be set in this area. The Minimum time is 10 seconds. When using either the Email or Authenticator, it is the time window you have to enter the code before it will time out.

LDAP Settings

LDAP (Lightweight Directory Access Protocol) securely manages users and their access rights to WMS Pro using its protocols in an active directory. To enable LDAP authentication, check the tick box. It will then provide a field for the Operator to enter a user's domain name, login name and password. The email address must match the email address of a User on the active directory.

Security

Password complexity

The password complexity requirements can be configured to the Operator's liking. By default, the password settings include a requirement for a: digit, lowercase character, uppercase character, non-alphanumeric (!#\$) character, and a required length of 8 characters.

Operator lock out

Operators can be locked out and denied further attempts to login after exceeding the maximum amount of failed login attempts. They can be manually granted permission to login again by selecting the "Unlock" action in the [Operators](#) page.

Maximum number of failed login attempt count before locking the account

The number of consecutive failed login attempts allowed before the Operator is "locked out" can be configured under this setting. It is set to 5 attempts by default.

Account locking duration (as seconds)

The locking duration refers to the length of time an Operator is prevented from logging in using their credentials as a result of them exceeding the maximum number of failed login attempts. The duration is set to 300 seconds by default.

Two factor login

Two factor authentication (2FA) is an identity and access management security method that requires two forms of identification to access resources and data. 2FA gives businesses the ability to monitor and help safeguard their systems.

To enable 2FA in WMS Pro, first tick the checkbox 'Enable two factor operator login', and a list of 2FA verification methods currently available in WMS Pro will be displayed. Tick the verification method(s) to be used with [Operator](#) logins, then click the 'Save all' button and refresh the page to enable the changes. Operators do not have 2FA enabled by default, so it's imperative that you also tick the 'Two factor authentication enabled' checkbox on any [Operator](#) that need to use 2FA.

Current supported 2FA verification methods include:

- Email - tick the 'Enable email verification' checkbox to have WMS Pro send a unique code to an Operator's email address when they attempt to login and have 2FA enabled on their account. Please note that email 2FA will only work once an [Operator's](#) activation email has been processed.
- Google Authenticator - When ticked, Operators with two factor authentication enabled will be able to authenticate with a One-Time Password (OTP) obtained from a compatible authentication app, such as Google Authenticator or Authy. To register WMS Pro in an authenticator app, Operators using this method will need to login to WMS Pro and access the 'My settings' section by clicking on the Operator profile menu located in the top right corner of WMS Pro. This will display a popup which displays an 'Enable authenticator app' option to guide the Operator through the simple 3 step process on their device.
- Allow to remember browser – If ticked the Operator can select to remember browser to skip second time two factor login for the same browser.

Email (SMTP)

Default from (sender) email address

Enter the default email address that will be labelled as the sender of the outgoing emails.

Default from (sender) display name

Enter the display name of the default email addressed used to label the sender of outgoing emails.

SMTP host

Enter the SMTP server that will process outgoing emails.

SMTP port

Enter the desired SMTP port. The default port is 587.

Use SSL

Tick to enable encryption.

Specify the **Domain name**, **Login name** and **Password** to authenticate with the SMTP server.

Test Email Settings

Send a test email to the email entered in this field. SMTP settings must be provided to initiate a test.

Note: The SMTP settings are required to enable WMS Pro to perform password resets when an Operator forgets their password.

Others**Database Maintenance****History log retention (Number of days to keep, 0 = no limit)**

DB maintenance allows the Operator to choose how long a History log can be retained for. (Number of days to keep, 0 = no limit) Use the up and down arrows to select the number of days. For example: 90 days = 3 months.

Transaction log shrink trigger in GB (minimum 1GB)

Transaction log shrink trigger Default is 10 GB. If current log exceeds trigger size, the system automatically shrinks the log file to the target size and creates an audit log entry. Background service monitors and maintains size automatically on start up and every hour of operation.

Transaction log shrink target in GB (minimum 1GB)

Transaction log shrink target Default is 4 GB. See above notes.

Cardholder

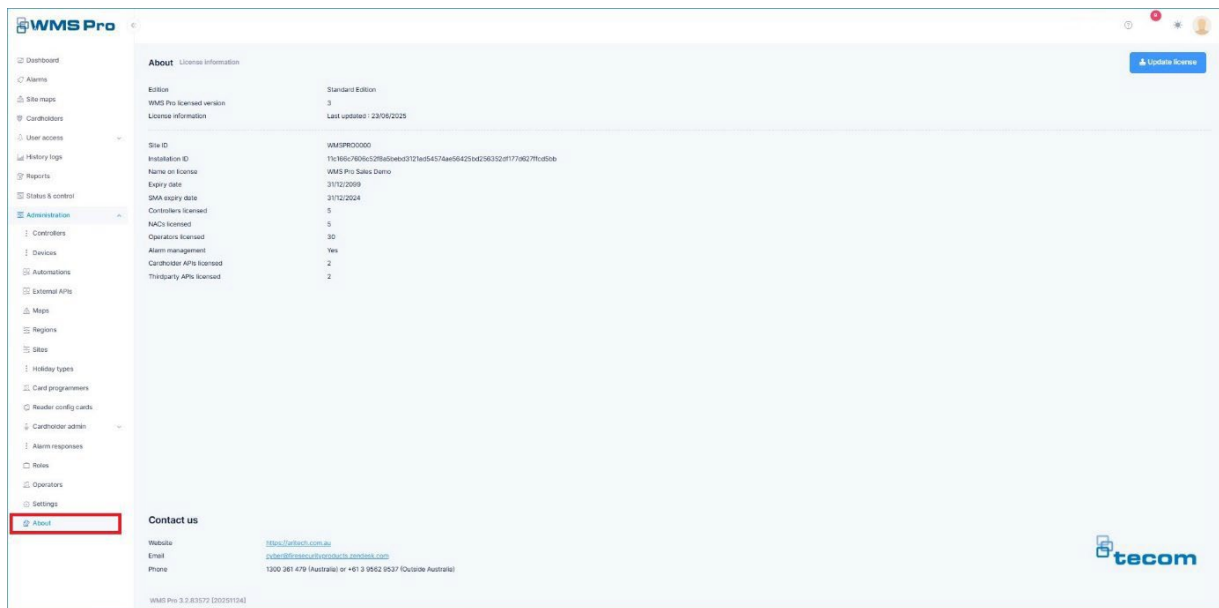
Checkbox to 'Allow view PIN' enables Operator to view Cardholder's PIN. The Operator's role Permissions also needs to include 'View saved PIN' in order to see the 'View PIN' option when editing a Credential.

**Save all**

Save the current configurations made in the Settings page.

About

License information



This page will display information about your installation; the licenses currently applied and contact information.

Every new installation starts with a 60 day trial license which includes 5 Controllers and 5 Operators.

Your site will need to be licensed before this trial ends in order to continue using all features of the software. If your license expires you will still be able to log in, but all panel comms will be disabled until a valid license is applied.

The online registration form can be accessed by clicking [here](#), please contact your installer or distributor for more information about licensing.

Edition

Displays the current WMS Pro edition in use

WMS Pro licensed version

Displays the current version number of WMS Pro. If the text is **red** then the licensed version is out of date, this occurs when the license version number is below the WMS Pro version number. For example, license version number 1.x for WMS Pro version 2.x will result in the license number being red.

Note: WMS Pro version can be found at the bottom of the page.

License information

Provides the date of when the applied license was most recently generated, and may not reflect the date that the license was applied to the installation.

Site ID

This is an identifier for the Site being controlled. (requires an updated license with this option)

Installation ID

This is a unique identifier for the installation, it is automatically generated when WMS Pro is first installed.

Name on license

This is the name of the site. By default the name will be displayed as "WMS Pro License", once a full license has been applied the name will be updated to display the site name provided during registration.

Expiry date

This shows the date that the current WMS Pro license expires. Once the expiration date has passed, all Controller comms will cease until a new license with a valid expiration has been applied. A banner indicating the expiration of the license will also appear in the [Dashboard](#), this banner will be visible at the start of the expiry date.

For sites that have been registered and have applied a paid license to WMS Pro, the expiry date will be shown as 31st December 2099. This essentially allows the site to be registered for the complete life span of the system.

SMA expiry date

This field shows whether SMA (Software Maintenance Agreement) is currently active for this site, and the date that it expires/expired.

SMA is now an option for WMS Pro.

Controllers licensed

The number in this field indicates the maximum amount of [Controllers](#) that are licensed in the system. It is not possible to enrol additional Controllers once this threshold has been reached.

NACs licensed

The number in this field indicates how many NACs (Network Access Controllers) are licensed in the system. It is not possible to enrol additional NACs once this threshold has been reached.

Operators licensed

The number in this field indicates the maximum amount of [Operators](#) that are allowed to be in the system at any one time. There is no practical limit to how many Operators can be created, however there is a limit to how many Operators can be logged in simultaneously - this is what's referred to as floating licenses. There is a 'Reserved seat' function where there may be specific Operator's that must be allowed to be on the system when needed. So for example there may be 5 licenses and 2 Reserved seats. That means the 2 seats are always reserved and the other 3 seats can be used as floating licenses / seats for when needed.

Alarm Management

Indicates if the [Alarm](#) Management functionality has been enabled for the current license applied in WMS Pro.

A new license, with the Alarm management enabled, will have to be applied to gain access to the functionality.

Cardholder APIs licensed

Provides the maximum amount of [Cardholder APIs](#) that are licensed in the system. If there is zero cardholder api license then the External APIs page is not visible.

NOTE: If they have either APIs licensed, then the page is visible and loading page will show both Cardholder API tab and 3rd party API tab. Operator will only be able to create API's for the license that they have.

Thirdparty APIs licensed

Provides the maximum amount of [Thirdparty APIs](#) that are licensed in the system. If there is zero 3rd Party api license then the External APIs page is not visible.

Contact us

The Aritech website, email address and phone number can be found in this section. For any tech support related issues please contact your security installer or distributor.



Update license

The WMS Pro license can be updated by clicking the "Update license" button. This will display a new pop-up window containing the Installation ID and an empty field to insert the license signature.

This license signature is a long and complex string of characters and is unique to your installation and registration options. It is strongly recommended that the license signature be copied and pasted in its entirety to prevent any incorrect entry of this code.

Note: Internet access is not required for the licensing process.

WMS Pro Server & Manger

WMS Pro now has a Windows application that will operate alongside your WMS Pro installation. With this app you can check the status of the following back-end dependencies:

- WMS Pro Panel Service
- IIS (Internet Information Service Manager)
- MSSQL Database
- WMS Pro Event service
- RabbitMQ

The app also allows a Windows administrator to perform some basic troubleshooting, such as restarting services and testing database connectivity, whilst also displaying a log of any events that affect these dependencies, e.g. when a service starts or stops.

The WMS Pro Server Status & Manager app also acts as a watchdog for the IIS service, which may be affected by Windows Updates. Enabling the 'Auto restart IIS on failure' checkbox will ensure that this service is automatically restarted in the event that it stops unexpectedly.

This app has been designed to act as a handy diagnostic tool, ensuring your WMS Pro system stays up and running smoothly.

Note: Restarting the event service will cause the panel service to stop. The panel service will need to be restarted afterwards. Panel service indicated Red icon and stopped when the event service is restarted.