WMS Pro by tecom

WMS PRO QUICK START GUIDE

Version 4.0

ARITECH

GETTING STARTED

This guide assumes that WMS Pro has already been **installed**. If this is not the case, please complete installation first and return here when done. Refer to the **WMS Pro Installation Guide** for more information.

LOGGING IN

To log into WMS Pro, first open up a web browser and enter the WMS Pro server address that was selected during the installation
(e.g. https://ipaddress or https://computername).

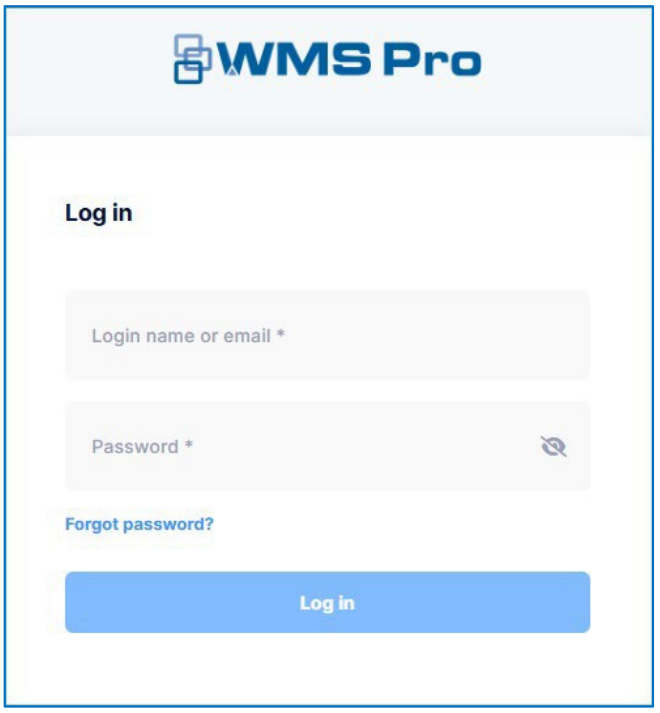
Note: WMS Pro address uses https only

If you are using a **self-signed certificate**, you will receive a warning when first accessing WMS Pro. On that warning page there should be an option to proceed ahead; this page is different for each browser.

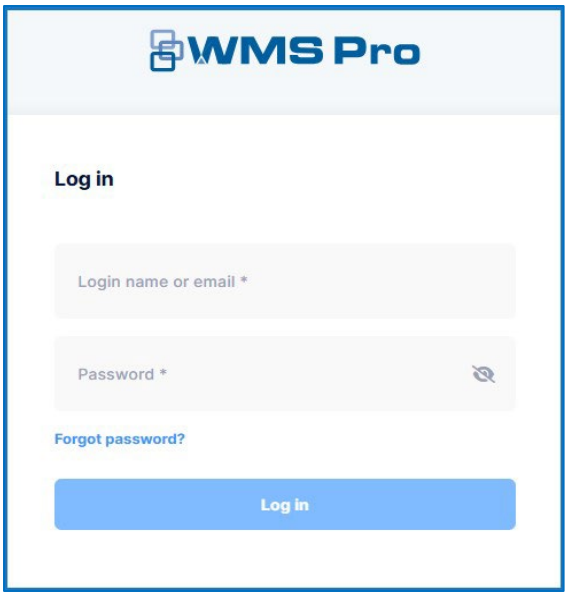
Once the login window appears, enter your login details in the given fields. The default credentials are:

Login name: admin
Password: Master#4346

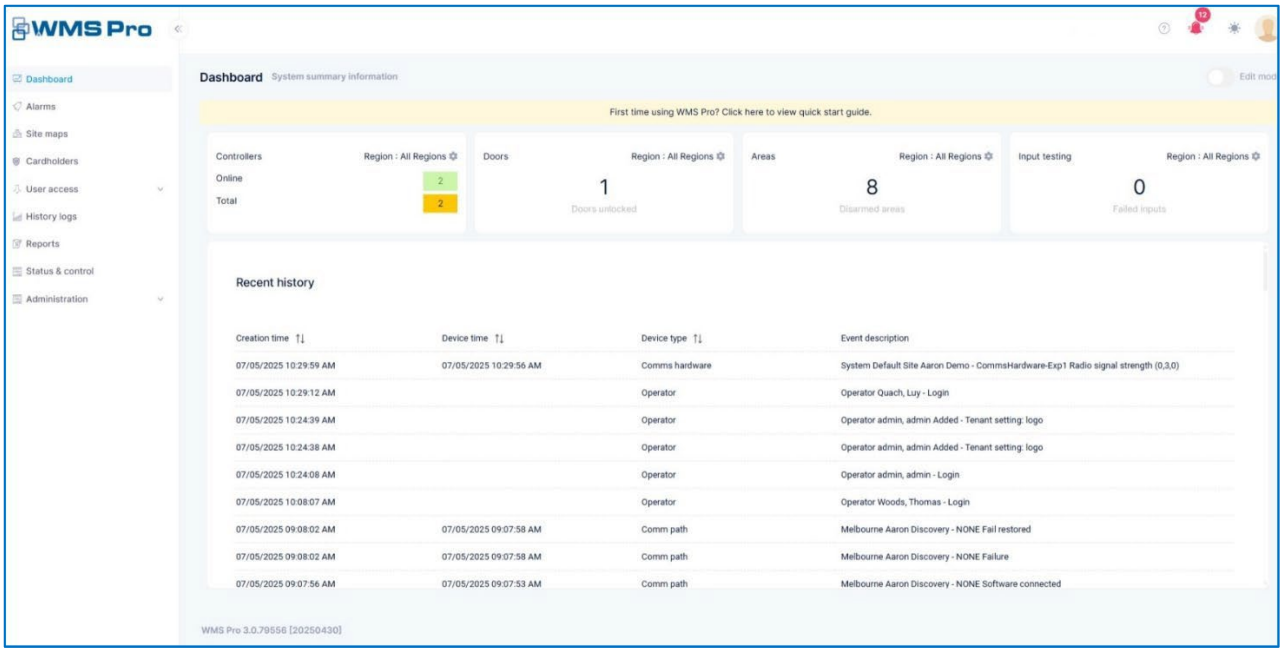
Note: Each Operator is restricted to a single active session. If multiple sessions are attempted with the same Operator credentials, then the previous active session will be logged off.



After you have successfully logged in for the first time, you will be prompted to change your password.



Once the password has been changed, you will be taken to the Dashboard page, as seen below.



ADDING A PANEL TO WMS PRO

Now that you've logged in and changed the default admin password, you can begin to get your hardware connected and online.

CONFIGURING PANELS TO COMMUNICATE WITH WMS PRO

When setting up communications to WMS Pro on your panel, you must first ensure the **Comm devices** are correctly configured, then configure a **Comm path** to the WMS Pro server.

Configuring a Discovery panel can be done using the **Discovery Web User Interface** (preferred) or **CTPlus,** whereas configuration of ChallengerPlus panels should only be performed via the **CTPlus** software. CTPlus must be version 3.0 or newer before proceeding, the download link can be found here: https://aritech.com.au/document-category/software/

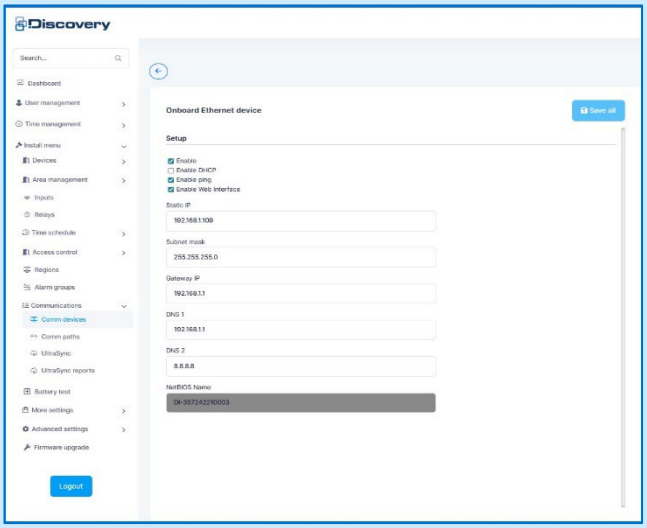
To find the IP address of your panel, use a keypad to navigate to menu 19 > 9 > 3 > 2 > 1. This menu will display some network configuration information, which can then be used to connect to your panel for the remaining configuration steps.

For Discovery panels, open a web browser and enter the displayed IP address to load the **Discovery WebUI**. To configure a panel in **CTPlus**, ensure it's either connected directly to a PC via USB (ChallengerPlus only), on the same network via Ethernet, or online via UltraSync.

To modify configuration of comm devices, refer to the below based on your preferred method:

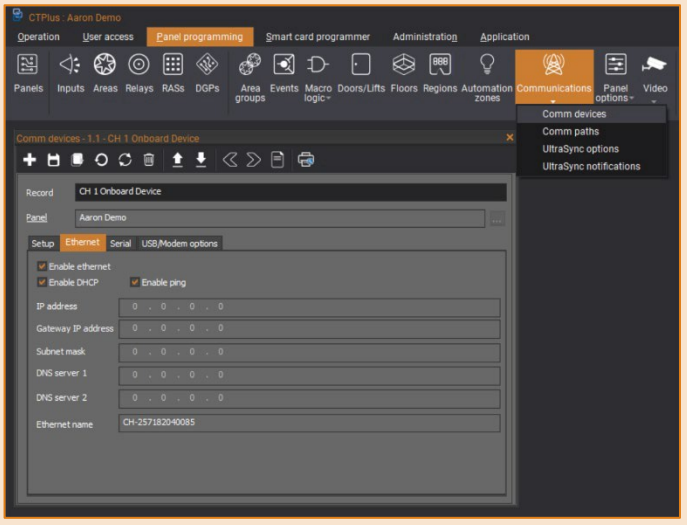
Discovery WebUI

Login and navigate to **Install Menu > Communications > Comms devices,** then select **Onboard Devices**.



CTPlus software

Login and navigate to **Panel programming > Communications > Comm devices**, and ensure the **Onboard Device** is selected.



To configure onboard Ethernet options, ensure the following are ticked or unticked as required:

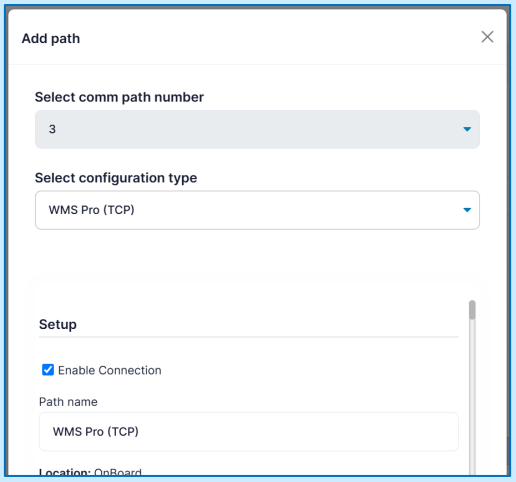
- **Enable ethernet** – when ticked, the onboard ethernet connection will be active.
- **Enable DHCP** – when ticked, the onboard ethernet connection will accept an IP address and other related network options from a DHCP server. Untick to set these options manually.
- **Enable Ping** – when ticked, the Discovery control panel will respond to ping requests on the onboard ethernet connection.

IP address info may be configured manually by ensuring that "Enable DHCP" is un-ticked, then filling in the required information. Please note that IP address and other network settings are not displayed here whilst DHCP is enabled.

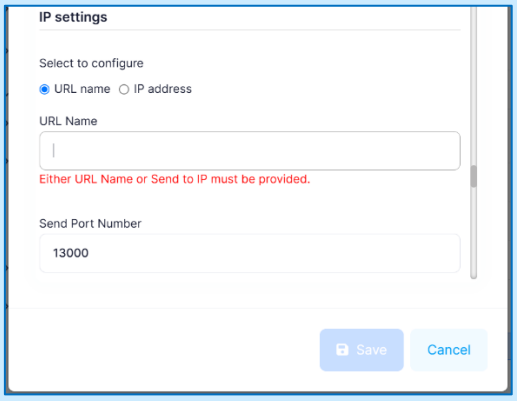
Once your panel has been configured with the appropriate network settings, it's time to set-up a comm path for connecting to WMS Pro. Refer to the below based on your preferred method:

Discovery WebUI

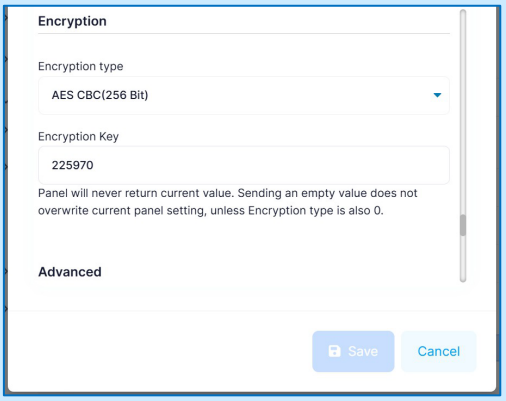
Navigate to **Install Menu > Communications > Comm paths**, then click the **+ Add** button in the top-right. Select an available comm path number, and select the configuration type called "WMS Pro (TCP)".



Scroll down until you reach 'IP settings', select either 'URL name' or 'IP address', and enter the IP address or domain name of the WMS Pro server, as entered during setup (https prefix not required).

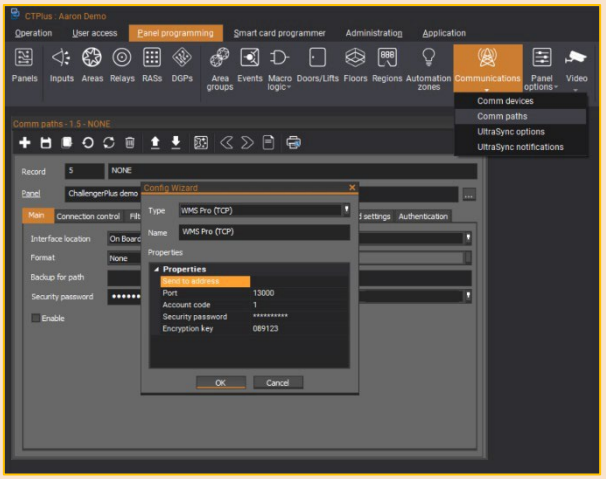


Scroll down again until you reach 'Encryption', and copy the 6-digit Encryption Key. ***You'll need this later.***



CTPlus software

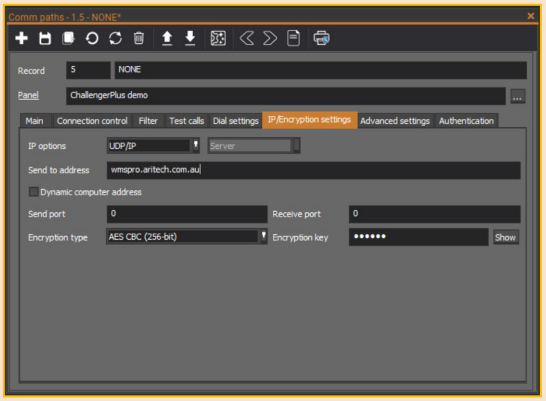
Navigate to **Panel programming > Communications > Comm paths**, then select an unconfigured path. Click on the **Config wizard** button, and select the type called "WMS Pro (TCP)".



Fill in the 'Send to address' field with the IP address or domain name of the WMS Pro server, as entered during setup (https prefix not required).



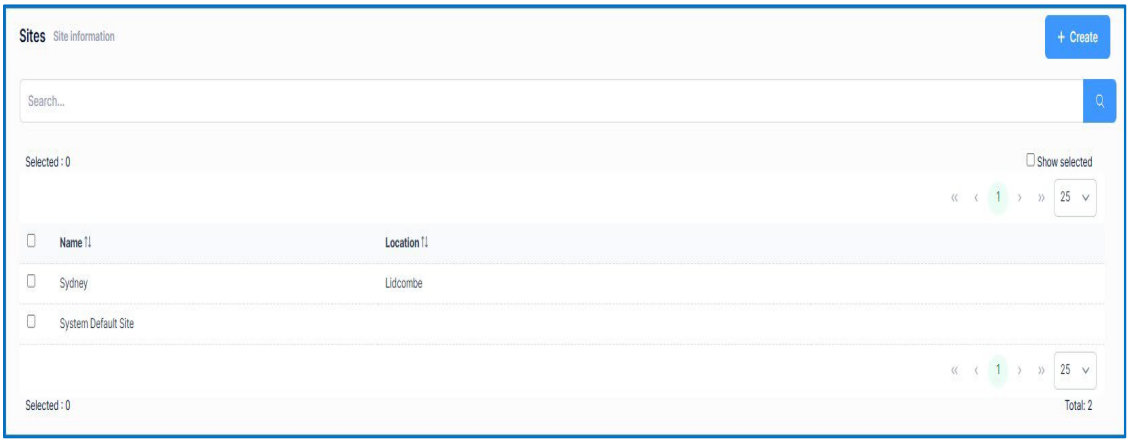
Copy the 6-digit Encryption key. ***You'll need this later.*** Settings can be changed at any time if required, on the **IP/Encryption settings** tab.



All other settings should be left at default values unless otherwise advised. Click the Save icon to finalise changes and activate the comm path. Once activated the comms path will start the handshake process with WMS Pro.

SETTING UP REGIONS AND SITES

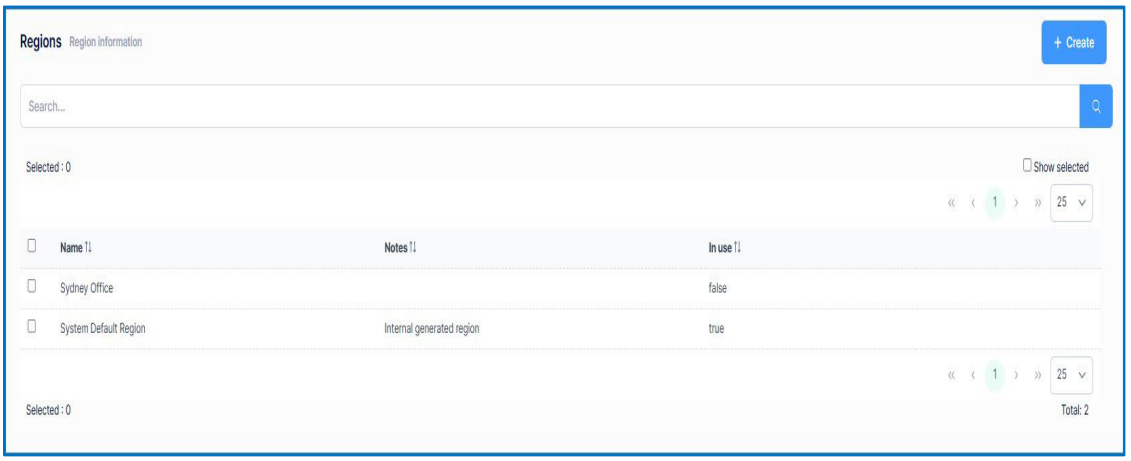
In WMS Pro, Sites are used to organise multiple Controllers into groups. These are typically used when Controllers are situated in the same location (e.g. if a large building contains multiple Controllers).



Regions are used for grouping multiple devices, and may span multiple Controllers. Regions can be created in any configuration with any device, and can impact what devices an Operator is able to see.

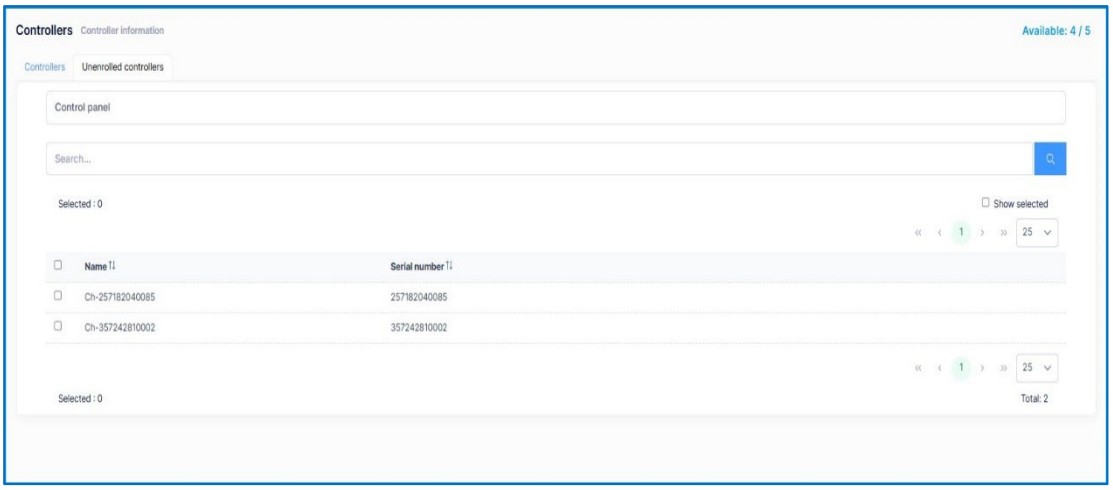
When enrolling a new Controller, you will be prompted to assign it to a Site and Region. By default there is already a **System Default Site** and **System Default Region** created in the system, which smaller installations may use in lieu of creating their own Site and/or Region organisational structures.

Note: All Controllers, Devices and Cardholders will be assigned to the Region specified during enrolment, which by default will be the **System Default Region**. Most items in WMS Pro must belong to at least one Region, and will be automatically reassigned to the **System Default Region** in the event that all assigned Regions are removed from the item(s).

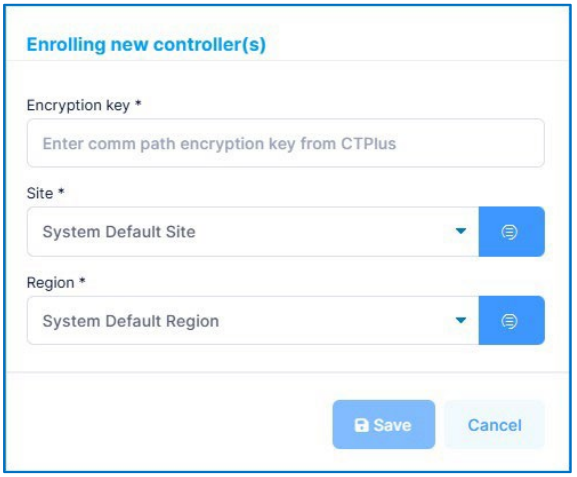


ENROLLING AN UNENROLLED CONTROLLER

Once the comm path record has been saved in the **Discovery WebUI** or **CTPlus**, the panel should now appear in WMS Pro under **Administration > Controllers > Unenrolled controllers**. You may have to select the appropriate Controller type from the selection list just above the search field.



Select the Controller to be enrolled, entering all required details in the pop-up window displayed. You will be prompted to enter the **Encryption key** from earlier, along with selecting the **Site** and **Region** to be assigned to this Controller, along with its Devices and Cardholders.



Use the **Enable** tickbox in the pop-up window to choose how the Controller is enrolled:

- **Ticked** – the Controller enrols and starts synchronising straight away.
- **Unticked** – the Controller is created but disabled, so you can configure it before it brings in any data.

Click "**Save**". If you left the Controller disabled, set its Credential groups, Region and any other required settings on the **Edit Controller** page, then tick **Enabled** and save.

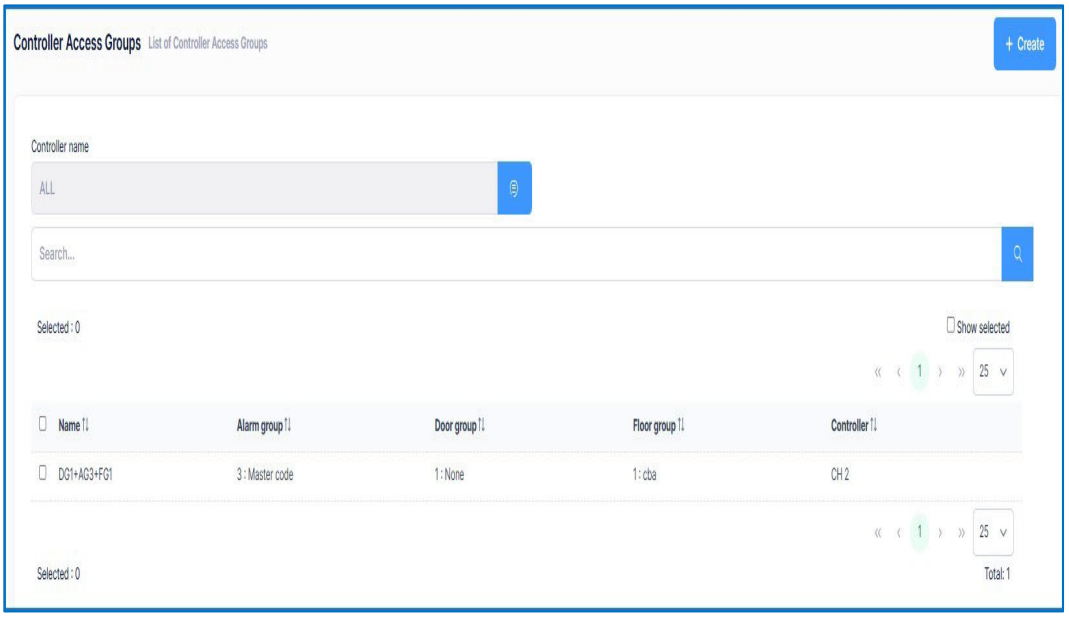
Note: Leave a new Controller disabled until its Credential groups, Region and other required settings are correct. Enable it once the configuration has been checked.

Once enabled, the Controller will start synchronising all programming and configuration into WMS Pro. This may take several minutes depending on the size of your system, and progress can be tracked on the Controllers page, the Status & control page, the Recent events widget on the Dashboard, or the History log page. Once completed, the Controller status will update from 'Retrieval in progress' to 'Online', and you will see an event or log entry saying "**Retrieve data complete**" for the Site and Controller name.

CONTROLLER ACCESS GROUPS

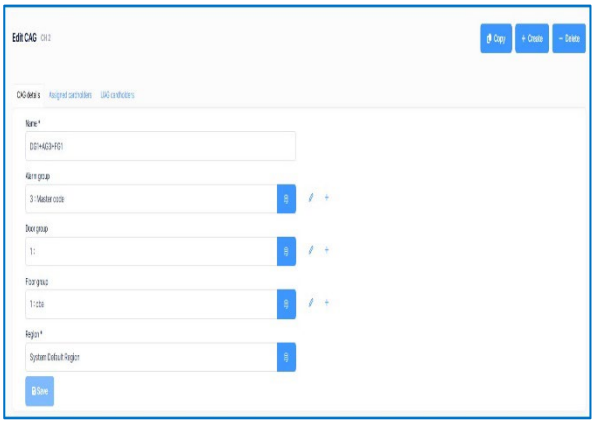
Controller Access Groups (CAG) are a unique combination of a Controller's alarm groups, door groups and floor groups that can be assigned to Cardholders in WMS Pro.

CAGs can be created manually and are also automatically generated from a pre-existing user's alarm, door, and floor groups. The names these generated CAGs are given follow the format "DGx+AGy+FGz" (Door Group + Alarm Group + Floor Group), examples of which can be seen below.



In the example to the right, this CAG has:

- Alarm group 32: "General staff arm/disarm"
- Door group 6: "Melbourne staff doors"
- Floor group 2: "Base building floor access"



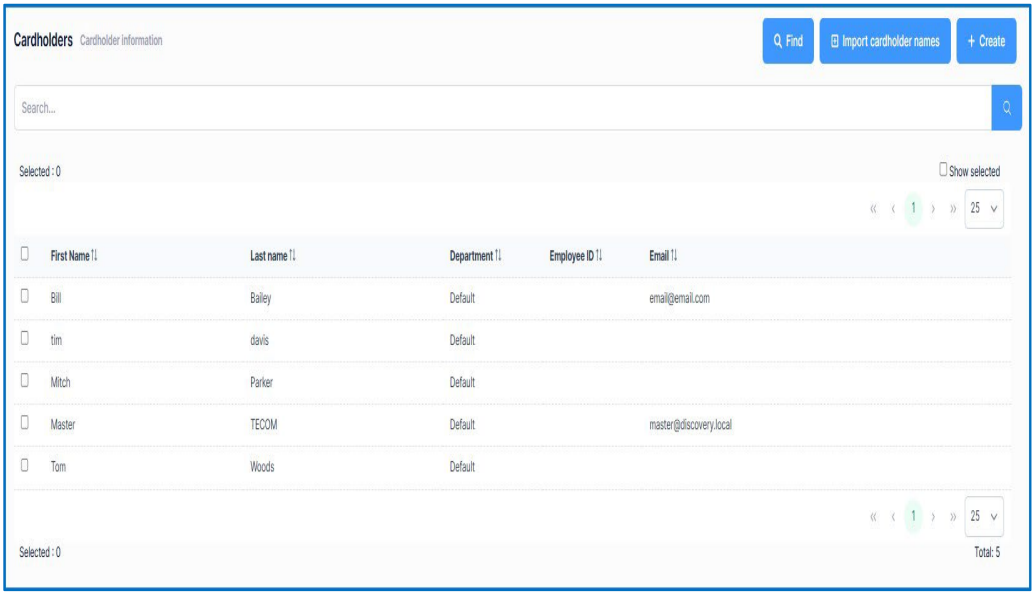
These three groups are all bundled together into a single CAG and can be assigned to multiple Cardholders.

Note: CAG name and groups can still be changed in the "Edit CAG" page, even after creating the CAG. Make sure the CAG name is meaningful and appropriate to the allocated groups.

CARDHOLDERS AND ASSIGNING ACCESS

A list of Cardholders can be found on the Cardholders page. In WMS Pro, a Cardholder is a person who has access to the physical system (e.g., accessing doors, arming/disarming areas, etc.) via means such as a card and/or PIN code.

New Cardholders can be created on this page, and pre-existing ones can have their details configured here. New Cardholders are automatically added to this list during Controller enrolment, using the information stored directly in the connected Controllers.

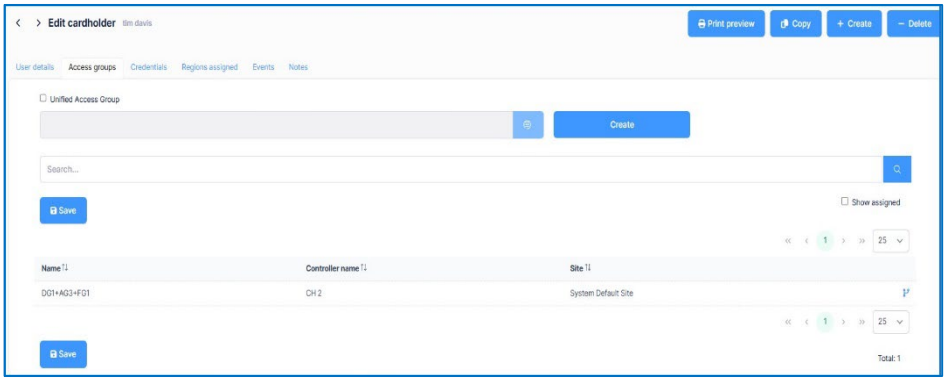


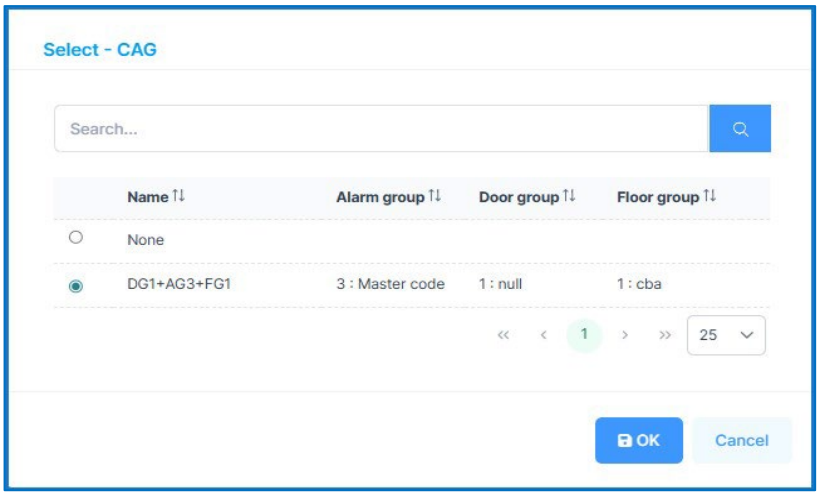
Please note:

- When there are multiple Controllers which have had their Cardholders and access groups brought into WMS Pro, there may be multiple “MASTER Tecom” Cardholders in the system. However, if all the MASTER Tecom Cardholders have the same card data, then WMS Pro will merge them all into a single Cardholder record. When enrolling multiple Controllers, it’s always recommended that installers ensure that identical card data is entered for common users such as MASTER Tecom.

- Cardholder names will be generic when retrieved from a Controller with an IUM fitted, as names are not stored on device hardware when fitted. Cardholders, including their names, can be imported at any time from a CSV file using the ‘Import’ button.

Cardholder details can be edited by clicking on the row containing the Cardholder name. Make sure to **always save** changes after entering details before moving to a new tab. To allocate **CAGs** to the Cardholder, click on the **Access groups** tab, then click the symbol in the Controller row to display a pop-up window allowing a CAG to be selected for that Controller.



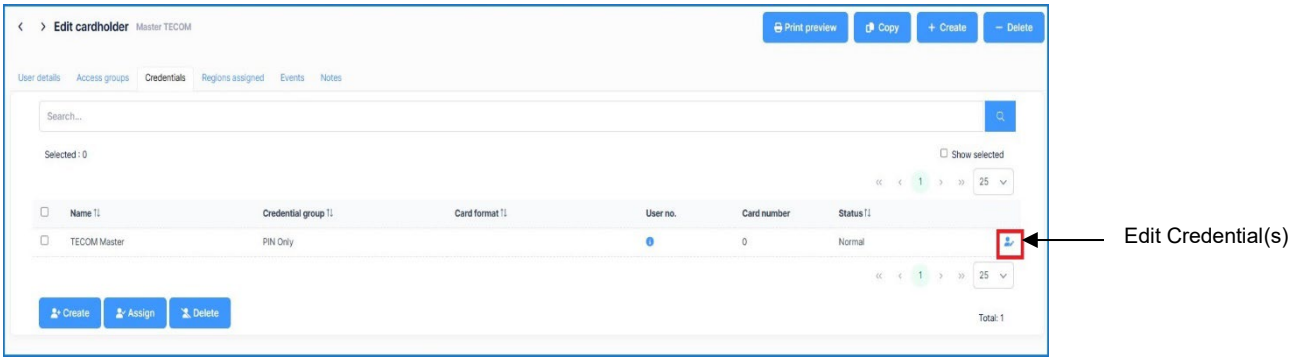


Select the desired CAG from the list then click "**OK**" to finalise the changes. Each Cardholder can only have one CAG per Controller assigned to them.

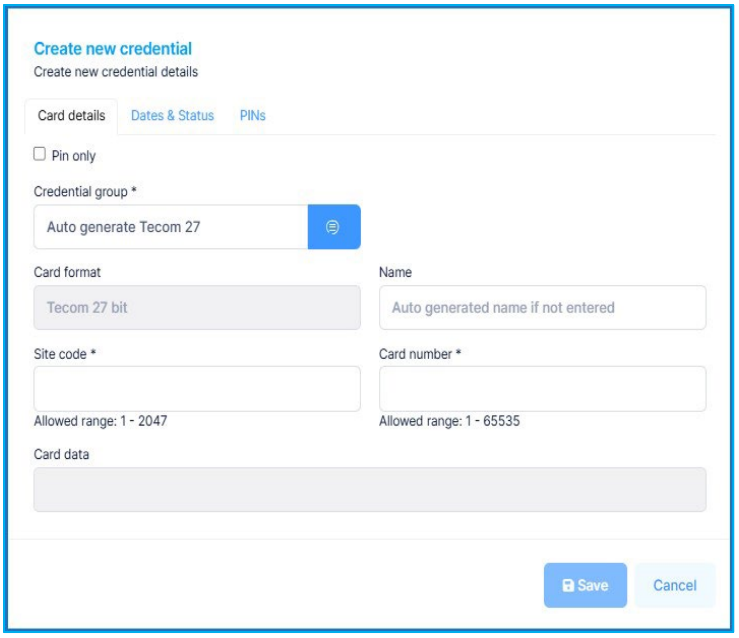
To quickly and easily assign access across multiple Controllers, **Unified Access Groups** (UAG) may be utilised. For more information about UAGs, see the embedded help menu in WMS Pro.

CREDENTIAL GROUPS

A Cardholder's Credentials can be configured in the **Credentials** tab. If there are pre-existing Credentials for the Cardholder, they will appear in the Credentials list. A new Credential may be created by clicking on the icon.



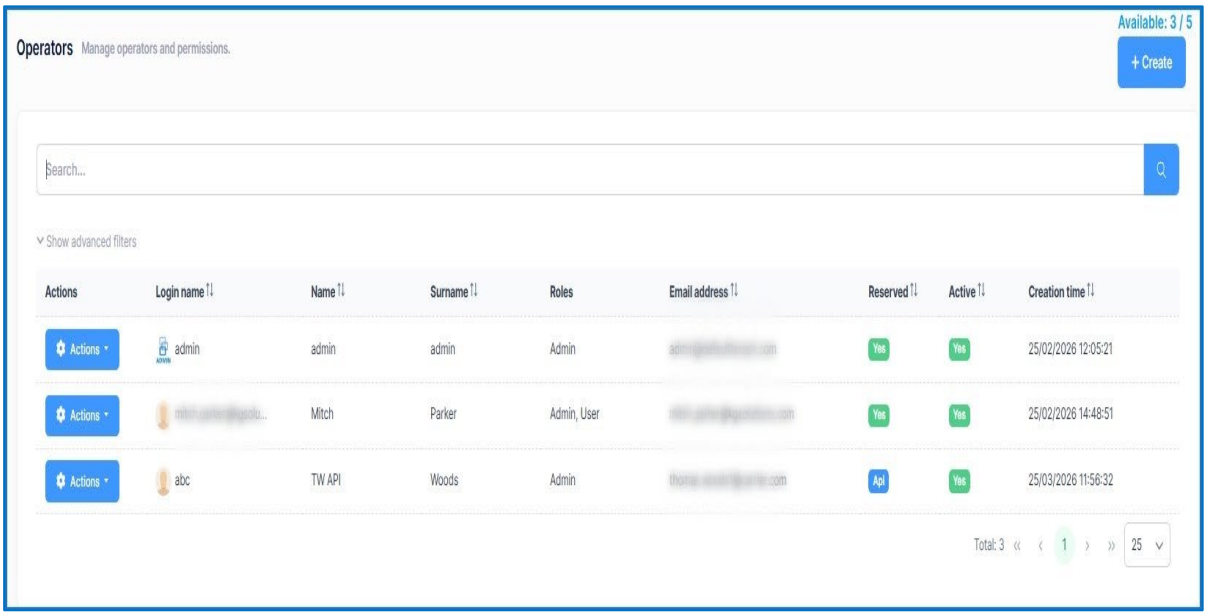
A new pop-up window will appear when a new Credential is being made. Selecting the **Credential group** will automatically populate the **Card format** field. The Credential group is what helps WMS Pro determine which Cardholder belongs to which Controller – as long as both of them share the same Credential group, the Cardholders' details will be sent to that Controller. For more information see the embedded help menu in WMS Pro.

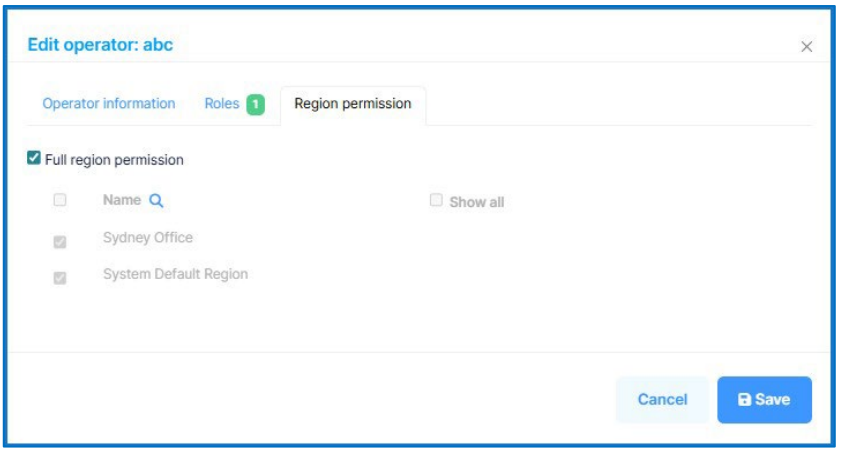


OPERATORS AND ASSIGNING REGIONS

Multiple Operators can be created in WMS Pro. To assign Regions to the Operators, navigate to Administration > Operators, click on the **Action** drop-down menu, select **Edit** to open a new pop-up window, go to the **Region permission** tab and tick the checkboxes next to each Region that Operator should have access to, or click on 'Full region permission' to allow access to all Regions created now and in the future. By assigning Regions to Operators, anything outside their assigned Regions is invisible to them, creating a closed and segregated system.

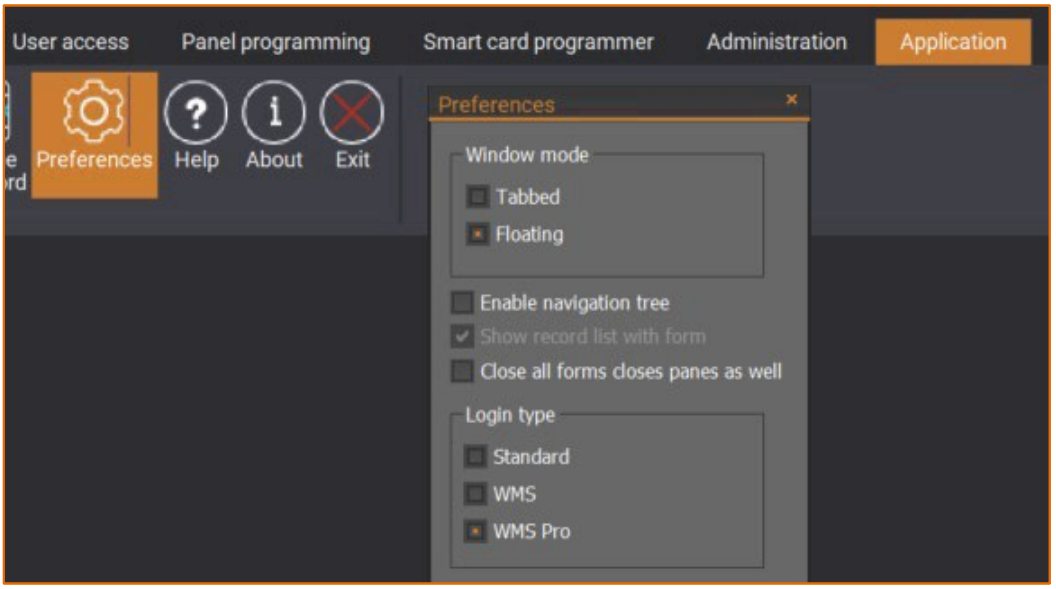
Devices are always assigned to at least one Region. Make sure devices are assigned and unassigned to their required Regions to make best use of this functionality.



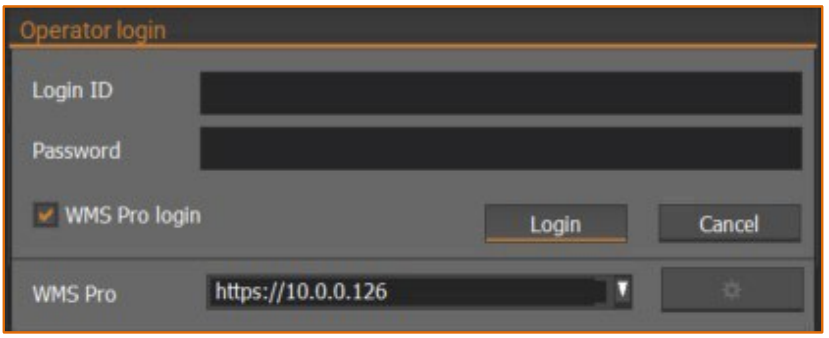


LOGGING IN THROUGH CTPLUS

Operators needing to make programming changes to Controllers and Devices can use CTPlus in "WMS Pro mode". This mode allows CTPlus to log in to the WMS Pro system rather than using the standard offline database, in order to access the programming data directly from the WMS Pro database. You will need to enable this functionality in CTPlus by navigating to **Application > Preferences** and selecting **WMS Pro** under **Login type**.



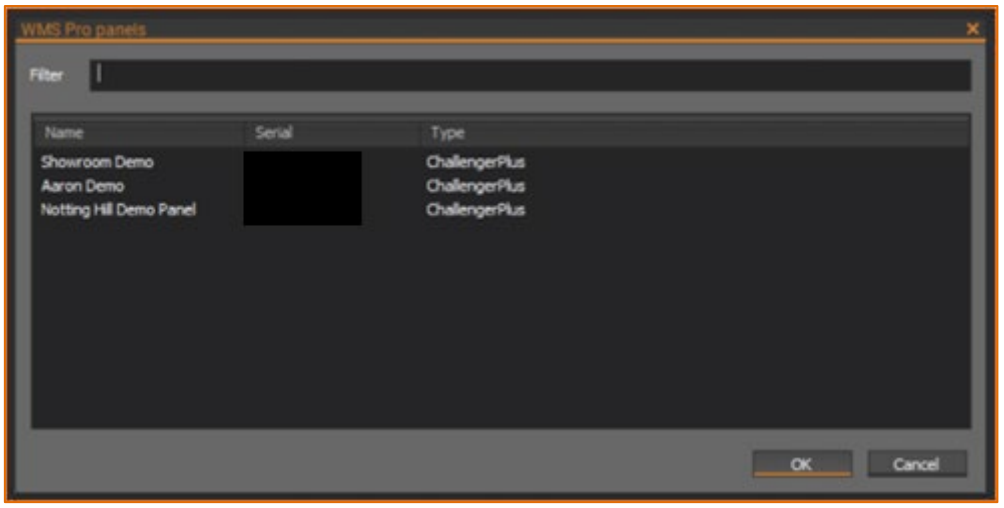
Once selected, click OK to save and logout of CTPlus. The next time you're presented with the CTPlus login screen, you'll see a new **WMS Pro login** option. Tick this option and enter your WMS Pro Operator login credentials in the **Login ID** and **Password** fields, and enter the address of the WMS Pro server (including the https prefix) to proceed.



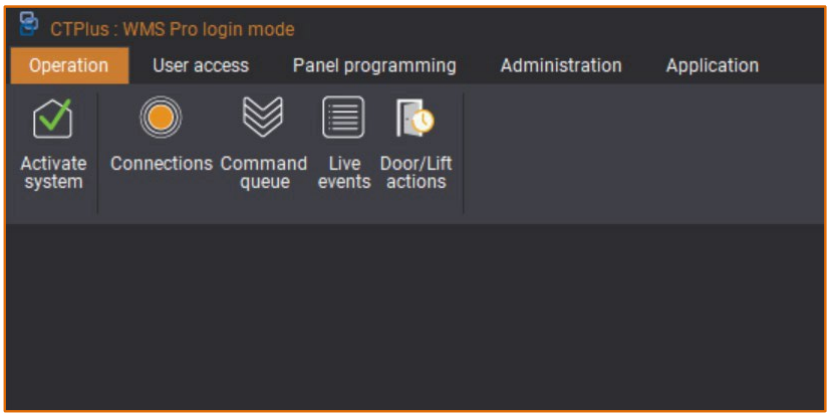
The WMS Pro address is the same as the one used for the WMS Pro installation, and as accessed by the web browser.

Note: The same operator credentials cannot be used simultaneously in both WMS Pro and CTPlus, it is strongly recommended that a unique Operator is created in WMS Pro for use with CTPlus.

When you have successfully logged in you will be presented with a list of panels enrolled in WMS Pro, select one to continue.



CTPlus is now using the WMS Pro database instead of the local CTPlus database. On the top left corner of CTPlus it will now say "**WMS Pro login mode**".



When using CTPlus in WMS Pro mode:

- Panel programming is immediately loaded and available to the installer
- Changes made are saved immediately in WMS Pro and the hardware
- Any changes made in CTPlus while connected to WMS Pro will automatically save the changes to both WMS Pro and the selected Controller.

To program a different panel in WMS Pro, click on the "**Activate system**" button (as seen in the above image) and select the desired panel from the available list. To switch back to the standard offline CTPlus database, logout and untick the "**WMS Pro login**" checkbox on the login window, then log back in using your normal CTPlus username and password.

TROUBLESHOOTING

The following information can be used for basic troubleshooting prior to contacting technical support. For further assistance with these or any other issues, please contact your system integrator or Tecom distributor.

UNABLE TO CONFIG CARDS USING CARD PROGRAMMER

If you have upgraded from WMS Pro 1.0, you will also need to upgrade the SCP Interface application from V1.0.0.2 to V1.0.0.4. If you are using WMS Pro 2.0 or later and still have SCP Interface V1.0.0.2, the card programmer can go online with WMS Pro but it will not be able to change config or write config/user cards.

To upgrade your SCP Interface follow these recommended steps on each PC with the SCP Interface installed:

- Uninstall SCP Interface
- Login to WMS Pro browser and go to Card programmers page
- Select card programmer to edit
- Press 'Download' to get the latest SCP Interface
- Unzip it and install the latest ScpInterfaceSetup.exe

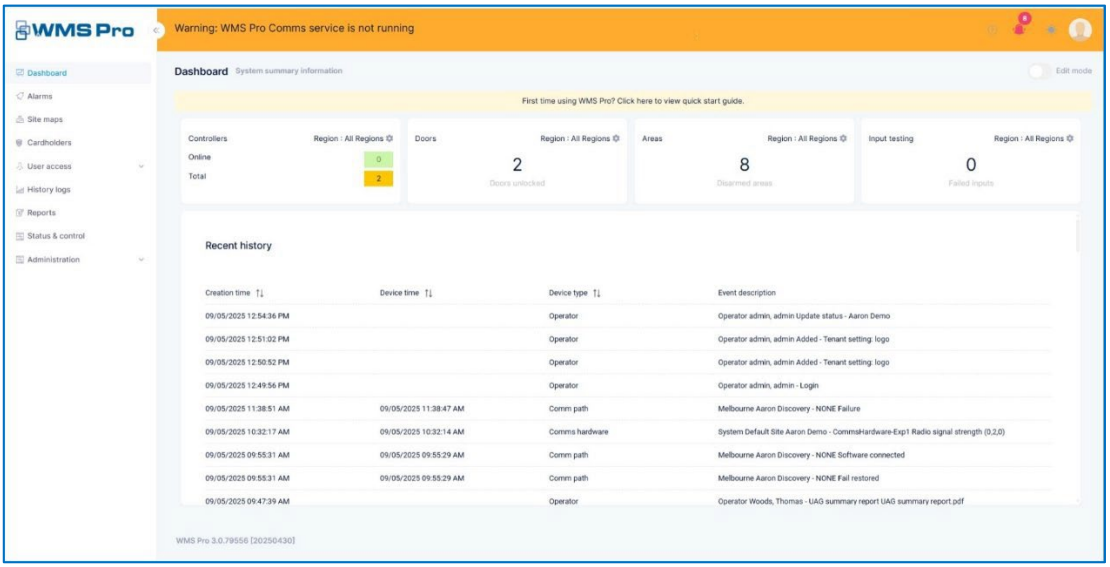
HOW RETRIEVING USER DATA IS IMPACTED BY THEIR CREDENTIALS

If user data is retrieved from a Controller already enrolled in WMS Pro and has different card data/user flags/start and end dates than what is found in WMS Pro, then the following will happen:

- If the card data belongs to a Credential group which is assigned to more than one Controller, a mismatch is detected.
- When a mismatch is detected, a mismatch event will be logged in history, and the current card data in WMS Pro will be sent back to the Controller, overwriting the user data in the panel so that it matches the data present in WMS Pro.
- If no mismatch is detected, then the changes from the Controller are applied to WMS Pro.

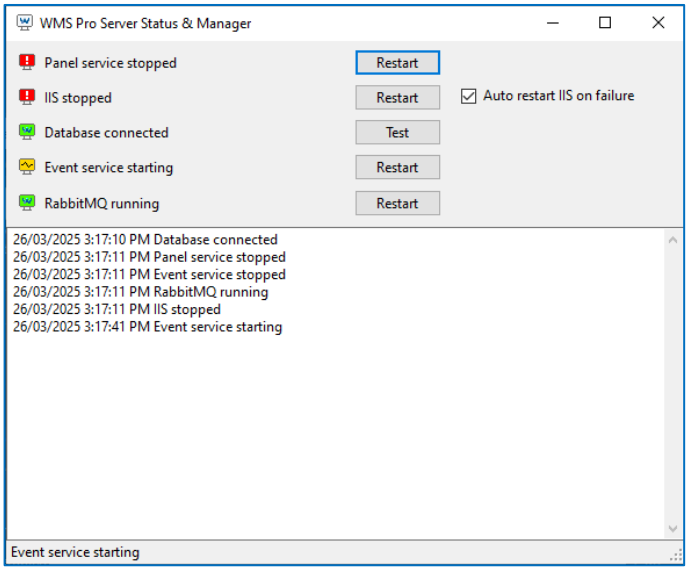
COMMS SERVICE IS OFFLINE

When the WMS Pro comms service is offline, an error message will appear to Operators currently logged in or attempting to log in to WMS Pro. Operators will not be able to use WMS Pro until the service is successfully restarted.



If this occurs, open the "WMS Pro Server Status & Manager" and attempt each of the steps below until your system is back online:

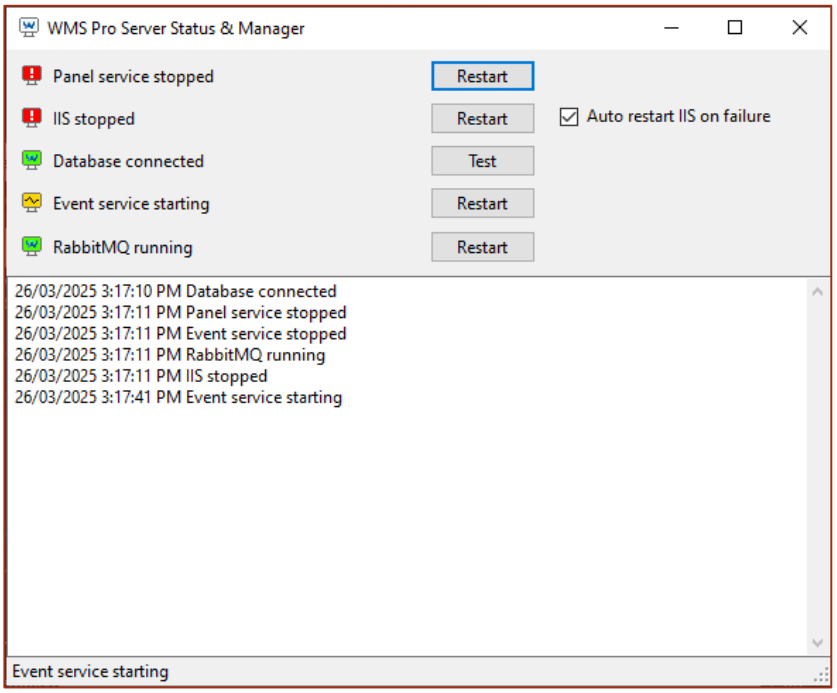
- Restart the Event service
- Restart the Panel service
- Restart IIS (Internet Information Services)
- Test that the database is connected.



Alternatively, the above services can also be managed or restarted via the Windows "Services" snap-in. Once all services have been successfully restarted, the error message should no longer appear and WMS Pro should continue to operate normally.

UNRESPONSIVE PANELS

In WMS Pro, you may encounter an issue where WMS Pro cannot communicate with Controllers, even though everything else seems to be working. This could be due to an issue with the WMS Pro comms service, where the service may indicate that it is running when in fact it isn't, or it might be stopped. Restart the panel service using the WMS Pro Service Status & Manager app.



Using a unique instance name instead of the default SQL server instance names, may also affect communications between WMS Pro and Controllers in some cases. Please contact your system integrator or local Tecom distributor for further assistance with this issue.

WMS Pro by tecom

WMS Pro Security Solutions

SCAN ME

Aritech Australia Pty Ltd
KGS Fire and Security
Australia Pty. Ltd.
Suite 4.01, 2 Ferntree Place
Notting Hill, Victoria 3168
Phone: 1300 361 479
www.aritech.com.au

Specifications subject to change without notice.

Aritech Australia Pty Ltd

©2026 Aritech, All rights reserved.
All trademarks are the property of their respective owners.

ARITECH