

WMS PRO QUICK START GUIDE

Version 2.3

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

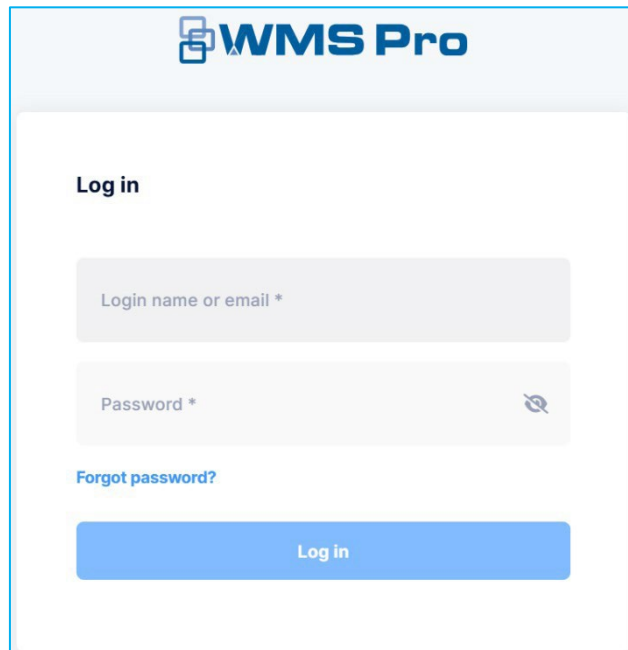
If you are using a **self-signed certificate**, you will receive a warning when first accessing WMS Pro. On that warning page there should be an option to proceed ahead; this page is different for each browser.

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.

The image shows the WMS Pro login interface. At the top, there is a header with the WMS Pro logo, which consists of a blue square icon with a white 'W' and the text 'WMS Pro' in blue. Below the header, the main content area is white. It starts with the text 'Log in' in bold. There are two input fields: the first is labeled 'Login name or email *' and the second is labeled 'Password *'. The password field has a blue eye icon to its right. Below the password field, there is a blue link that says 'Forgot password?'. At the bottom, there is a large blue button with the text 'Log in' in white.

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



Change password

Please enter your new password.


Password

Password (repeat)

← Back

✓ Submit

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



Dashboard

Alarms

Cardholders

User access

History logs

Reports

Status & control

Administration

Dashboard

System summary information

First time using WMS Pro? Click here to view quick start guide.

Controllers

Region: All Regions

Online

1

Total

4

Doors

Region: All Regions

1

Doors unlocked

Areas

Region: All Regions

20

Disarmed areas

Input testing

Region: All Regions

0

Failed inputs

Recent history

Creation time	Device time	Device type	Event description
29/10/2024 10:32:22 AM		Operator	Operator admin, admin - Login
29/10/2024 10:50:17 AM		Operator	Operator admin, admin - Logout
29/10/2024 10:34:14 AM		Operator	Operator admin, admin Added - Floor group: Notting Hill Demo Panel General Staff Floors Only
29/10/2024 10:33:56 AM		Operator	Operator admin, admin Modified - Floor group: Notting Hill Demo Panel All Floors 24/7 [Field:"Name", "Old":"General Staff Floors Only", "New":"All Floors 24/7"]
29/10/2024 10:33:02 AM		Operator	Operator admin, admin Added - Door group: Notting Hill Demo Panel Melbourne_DG
29/10/2024 10:31:58 AM		Operator	Operator admin, admin Modified - Floor group: Notting Hill Demo Panel General Staff Floors Only [Field:"Name", "Old":"Office Area_FG", "New":"General Staff Floors Only"]

WMS Pro 2.2.76868 | API: v13.1.0 | Client: v13.1.0 [20241025]

ADDING A PANEL TO WMS PRO

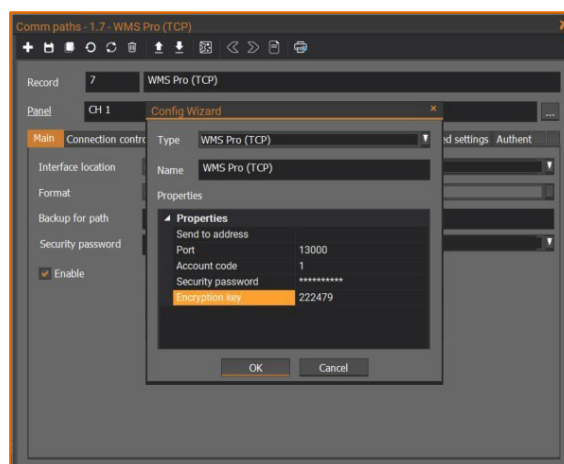
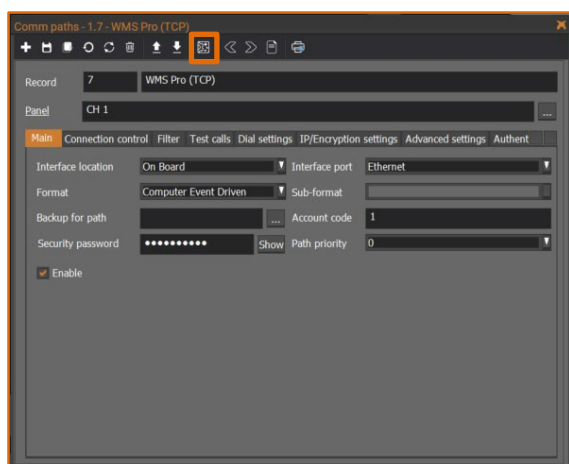
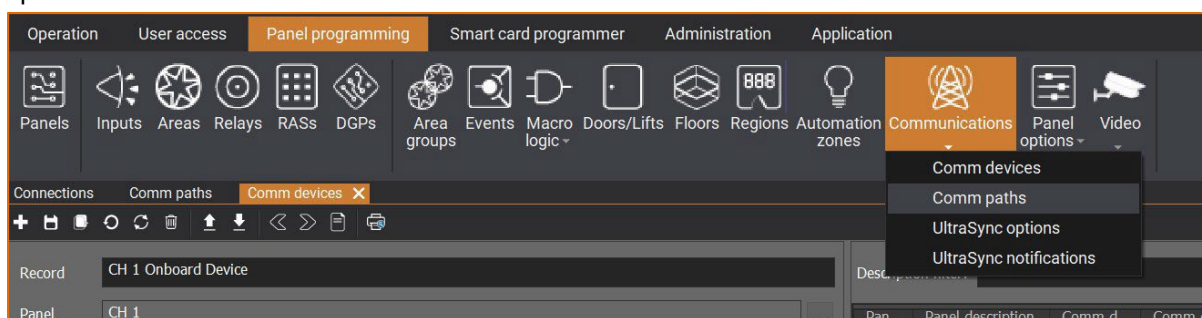
Once you have logged in and changed your default password, you can begin to get your hardware connected and online.

CONFIGURING THE PANEL TO COMMUNICATE WITH WMS PRO

The following steps take place in the **CTPlus** management software, the panel should be directly connected to the PC via USB, Ethernet, or UltraSync.

CTPlus must be version 3.0 or newer before proceeding, the download link can be found here: <https://aritech.com.au/document-category/software/>

Once you have your panel connected and communicating to CTPlus, click on the **Comm paths** option menu.



Select an **unconfigured** comm path (in the example above record 7 was chosen) from the record list, then click on the **Config wizard** button to bring up a new pop-up window, and fill in details:

- **Type:** WMS Pro (TCP)
- **Send to address:** Enter the IP address (or domain name, if applicable) of the WMS Pro server (https prefix not required)
- **Encryption key:** This is a 6-digit code that has been randomly generated by CTPlus. You will need to input this in WMS Pro when enrolling the panel, we recommend copying and/or writing this code down

All other settings should be left at default values unless otherwise advised. Click **OK**, then click the **Save** icon to finalise the 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: By default all Controllers, Devices and Cardholders will be assigned to the **System Default Region** and be accessible to all Operators until they are manually assigned different Regions. They must belong to at least one region, if they were manually unallocated from all Regions they will be automatically reassigned to the System Default Region.

Regions Region information + Create

Search...

Selected : 0 Show selected

<input type="checkbox"/> Name ↑↓	Notes ↑↓	In use ↑↓
<input type="checkbox"/> Lidcombe Distribution Warehouse		true
<input type="checkbox"/> Melbourne Head Office	Notting Hill	true
<input type="checkbox"/> Melbourne Warehouse		true
<input type="checkbox"/> System Default Region	Internal generated region	true
<input type="checkbox"/> test 1		true
<input type="checkbox"/> test 2		true

Selected : 0 Total: 6

Sites Site information + Create

Search...

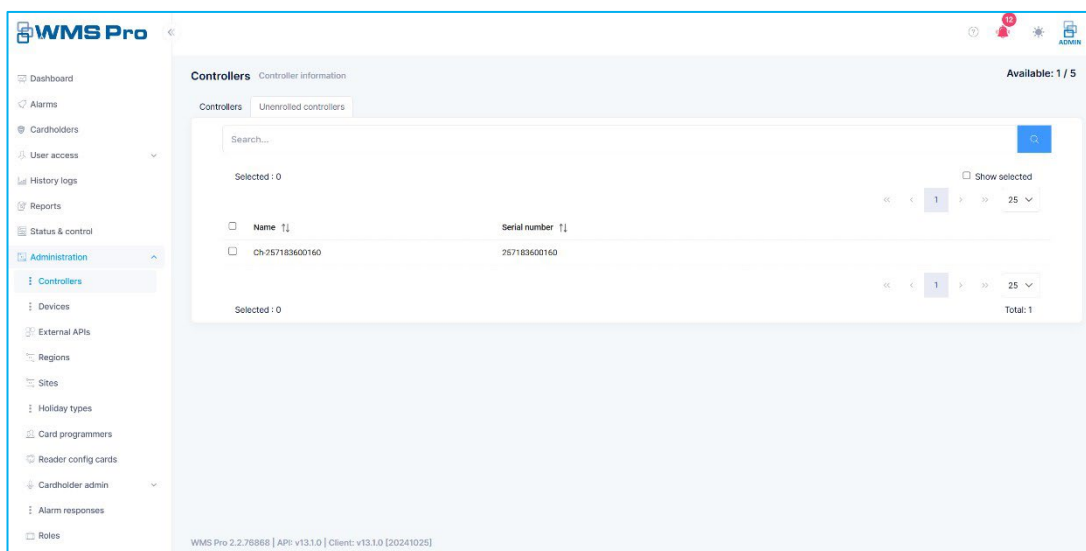
Selected : 0 Show selected

<input type="checkbox"/> Name ↑↓	Location ↑↓
<input type="checkbox"/> Melbourne	Notting Hill
<input type="checkbox"/> Sydney	
<input type="checkbox"/> System Default Site	

Selected : 0 Total: 3

ENROLLING AN UNENROLLED CONTROLLER

Once the comm path record has been saved in **CTPlus**, the panel should now appear in WMS Pro, under Administration > Controllers > **Unenrolled controllers** tab. Click anywhere in the row of the Controller you want to enroll, this will open a new pop-up window where the Operator will be prompted to enter the **Encryption key** and select the **Site** and **Region**. The **Encryption key** field needs to contain the same code you copied or noted down from the CTPlus steps on page 3.



Enrolling new controllers

Encryption key *

Site *

System Default Site

Region *

System Default Region

Save

Cancel

Enter the enrolment details, then click **“Save”** to finalise the enrolment.

If all details have been entered correctly, your Controller is now enrolled and should have already started synchronising all programming and configuration into WMS Pro. This process may take several minutes depending on the size of your system, and progress may be tracked on the Controllers page under Administration. Alternatively, you can view progress from the Recent events widget on the Dashboard, the History log page, or the Status & control page. Once completed, the Controller status will be Online, and you will see an event or log entry saying **“Retrieve data complete”** after the site and panel 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.

Name	Alarm group	Door group	Floor group	Controller
DG20+AG31	31 : Office Staff Alarm Group	20 : Office Staff Door Group	0 : None	Notting Hill Demo Panel
DG52+AG1	1 : No access	2 : Warehouse Staff DG	0 : None	Notting Hill Demo Panel
DG20+AG1	1 : No access	20 : Office Staff Door Group	0 : None	Notting Hill Demo Panel
DG1+AG1	1 : No access	1 : All Doors 24/7	0 : None	Notting Hill Demo Panel
DG3+AG32	32 : CH 2 Alarm Group 32	3 : Office Area_DG	0 : None	Notting Hill Demo Panel
AG13+FG1	13 : None	0 : None	1 : All Floors 24/7	Notting Hill Demo Panel
AG13	13 : None	0 : None	0 : None	Notting Hill Demo Panel
DG1+AG31	31 : Office Staff Alarm Group	1 : All Doors 24/7	0 : None	Notting Hill Demo Panel
Default Tecom Master CAG	3 : Master code access	1 : All Doors 24/7	0 : None	Notting Hill Demo Panel
Office Area	11 : Office Area_AG	3 : Office Area_DG	1 : All Floors 24/7	Notting Hill Demo Panel
DG2+AG30	30 : Carrier Staff AG	2 : Carrier Staff DG	0 : None	Showroom Demo

In the example to the right, this CAG has:

- Alarm group 11: "Area One"
- Door group 6: "Melbourne_DG"
- Floor group 9: "General Staff Floors Only"

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.

Edit CAG Notting Hill Demo Panel

Copy Create Delete

Name *

DG6+AG11+FG9

Alarm group

11 : Area One

Door group

6 : Melbourne_DG

Floor group

9 : General Staff Floors Only

Save

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.

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.

Note: Cardholder names will be generic when retrieved from a Controller with an IUM fitted, as names are not stored on hardware with IUMs fitted. A list of Cardholder names can be imported at any time by using the ‘Import cardholder names’ button.

WMS Pro

Cardholders Cardholder information


Search...

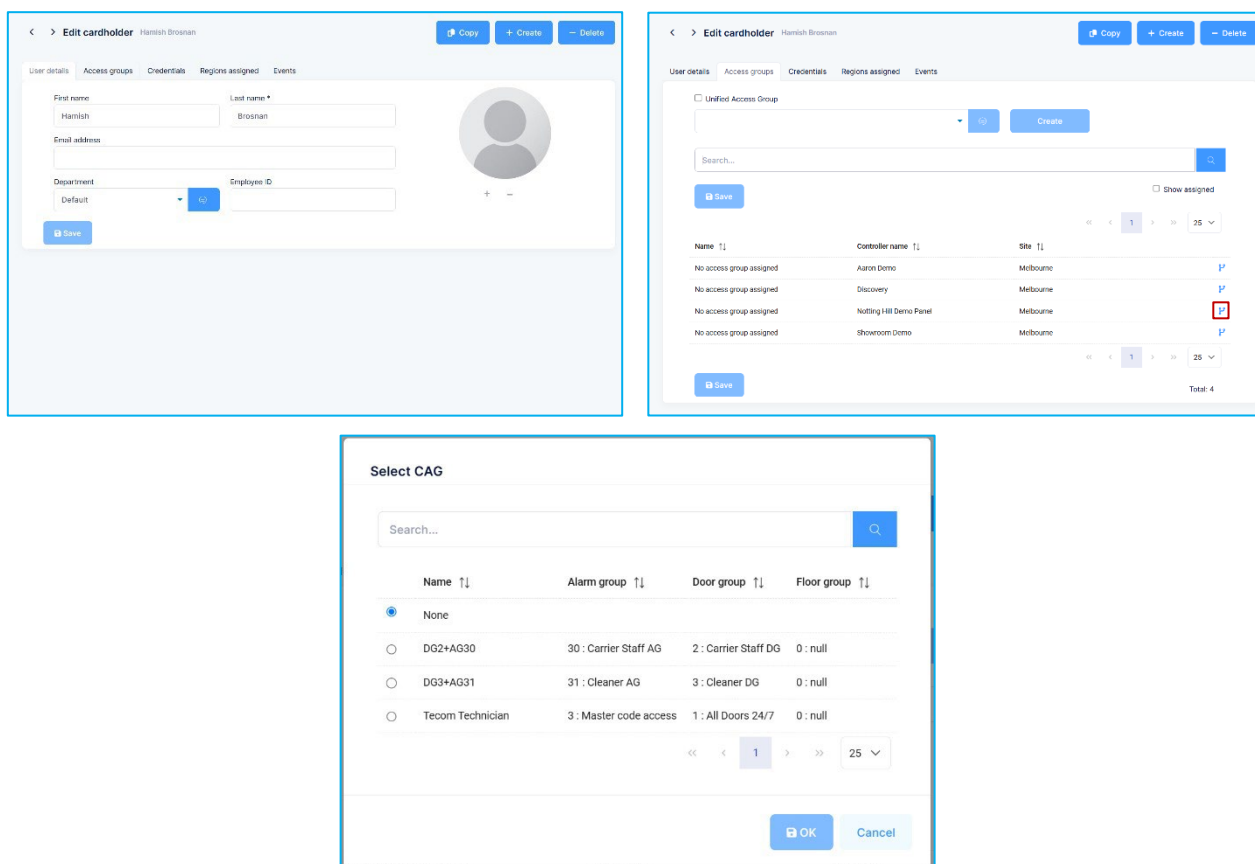
Selected: 0

<input type="checkbox"/>	First name [1]	Last name [1]	Department [1]	Employee ID [1]	Email [1]
<input type="checkbox"/>	Dennis	Bailey	Office Staff	100	dennis@vcorp.com
<input type="checkbox"/>	Georgia	Bennett	Default		
<input type="checkbox"/>	Hamish	Brosnan	Default		
<input type="checkbox"/>	Clin	Buchanan	Default		
<input type="checkbox"/>	Eleanor	Campbell	Default		
<input type="checkbox"/>	Aaron	Cargill	Default		
<input type="checkbox"/>	Aaron	Cargill	Default		
<input type="checkbox"/>	Ping	Chai	Default		
<input type="checkbox"/>	Ryan	Chen	Default		
<input type="checkbox"/>	Dean	Cherry	Default		
<input type="checkbox"/>	Profess	Cleaning	Default		
<input type="checkbox"/>	Ross	Conway	Default		
<input type="checkbox"/>	Tamsyn	Coombs	Office Staff		

1 2 3 4 5 >> 25

Show selected

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 open up a new pop-up window which will allow a CAG to be selected for that Controller.



The first screenshot shows the 'Edit cardholder' form for 'Hamish Brosnan'. The 'Access groups' tab is selected, and the 'Controller' row is highlighted with a key icon.

The second screenshot shows the 'Access groups' tab with a table of assigned CAGs. The 'Controller' row is highlighted with a key icon.


The third screenshot shows the 'Select CAG' pop-up window. It contains a search bar and a table of available CAGs. The 'None' option is selected.

Name	Alarm group	Door group	Floor group
None			
D62+AG30	30 : Carrier Staff AG	2 : Carrier Staff DG	0 : null
D63+AG31	31 : Cleaner AG	3 : Cleaner DG	0 : null
Tecom Technician	3 : Master code access	1 : All Doors 24/7	0 : null

Select your desired CAG from the list then click “OK” to finalise the changes. Only one CAG per Controller can be assigned to a Cardholder.

To assign multiple CAGs, each from a different Controller, **Unified Access Groups** (UAG) can be used instead. 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.

Program Credential
Edit Credential(s)
Assign PIN codes

Create Credential
Delete Credential

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.

Create credential(s)
Create new credential details

Credential group *
Auto generate Tecom27

Card format
Tecom 27 bit

Name
Hamish Brosnan

Start date
End date

User type *
Normal

Status *
Normal

Site code
1

Card number
2013

Card data
27.0.0.0.1.7.221

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

Save Cancel

OPERATORS AND ASSIGNING REGIONS

Multiple Operators can be created in WMS Pro, up to the limit available in the activated license. 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. 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 Regions if you want to make use of this functionality.

Operators Manage operators and permissions. Available: 32 / 50 [+ Create](#)


Search...

▼ Show advanced filters

Actions	Login name ↑↓	Name ↑↓	Surname ↑↓	Roles	Email address ↑↓	Active ↑↓	Creation time ↑↓
Actions	admin	admin	admin	Admin	admin@defaulttenant.com	Yes	2/8/2024, 3:42:01 PM
Actions	master	CTPlus	Software	Admin		Yes	2/8/2024, 3:46:49 PM
Actions	abc	Demo	API	Admin		Yes	10/7/2024, 4:15:16 PM
Actions	demoapi	Demo	API	Admin		Yes	3/8/2024, 1:30:23 PM
Actions	hugh.ogilvy	Hugh	Ogilvy	Admin		Yes	7/5/2024, 9:34:12 AM
Actions	luy.quach	Luy	Quach	Admin		Yes	6/21/2024, 11:59:36 AM
Actions	manasa.arravalli	Manasa	Arravalli	Admin		Yes	4/8/2024, 1:16:40 PM
Actions	meru.dharni	Meru	Dharni	Admin		Yes	2/21/2024, 2:38:42 PM
Actions	op2	Op2	Op2	Admin		Yes	4/8/2024, 1:17:11 PM
Actions	op3	Op3	Op3	Admin		Yes	4/8/2024, 1:17:35 PM

Edit operator: admin

Operator information Roles 1 Region permission

 **ADMIN**

Change profile picture

First name *
admin

Surname *
admin

Email address *
admin@defaulttenant.com

Phone number

Login name *
admin
Can not change login name of the admin.

Password

Password (repeat)

☐ Should change password on next login.

☐ Send activation email.

☒ Active

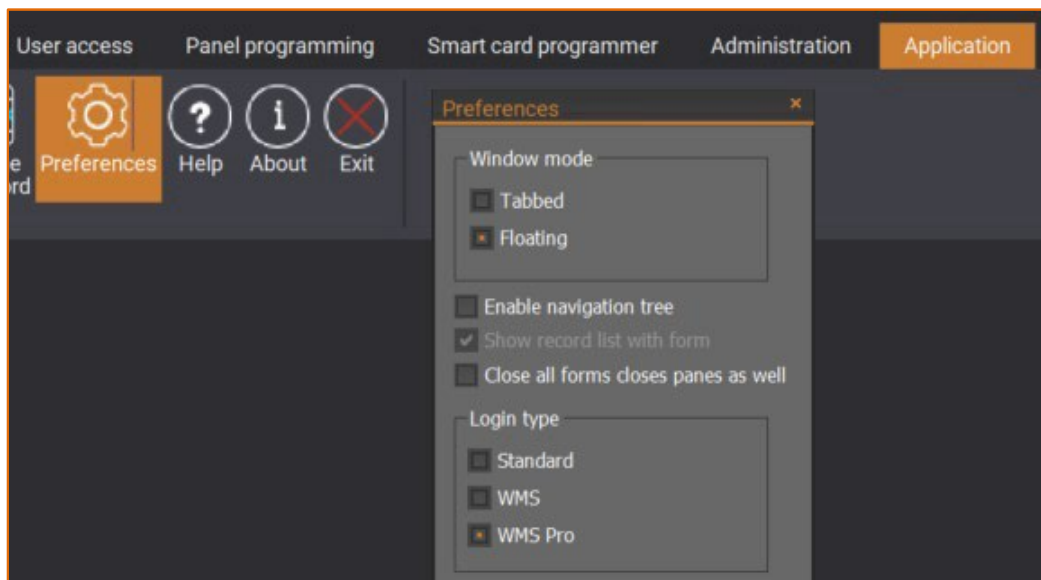
☒ Lockout enabled

☐ External API operator

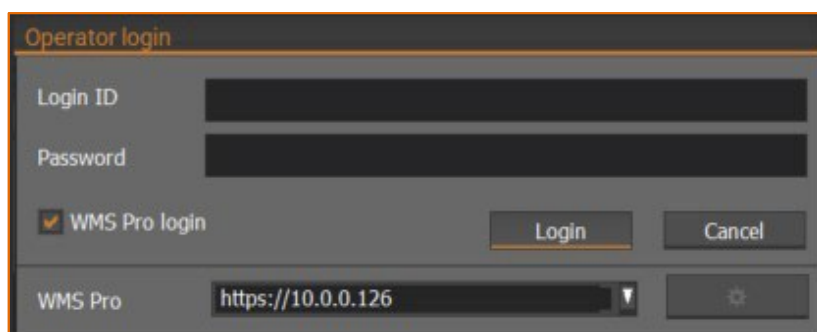
[Cancel](#) [Save](#)

LOGGING IN THROUGH CTPLUS

Operators can login to WMS Pro through CTPlus instead of using a web browser. You will have to enable this functionality in CTPlus by opening the **Preferences** option window and selecting the **WMS Pro** check box under **Login type**.



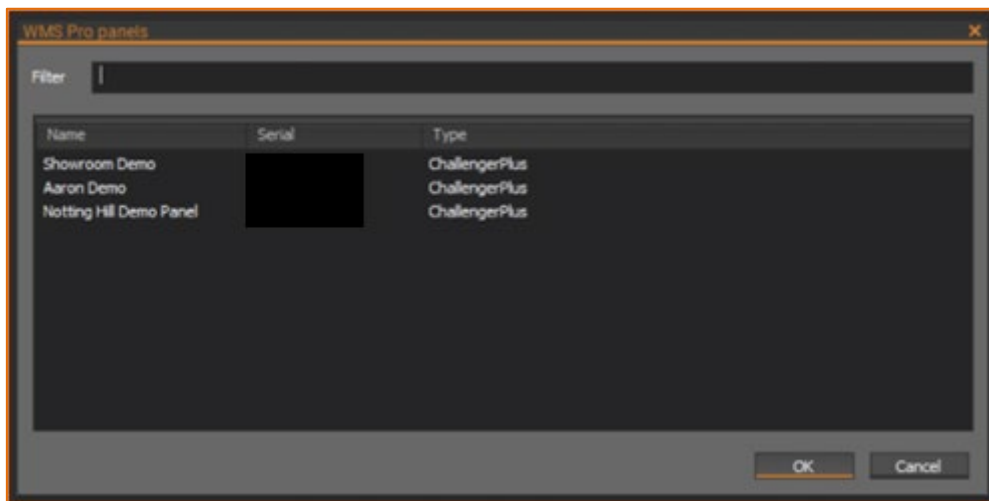
Logout of CTPlus, then log in again but with the **WMS Pro login** option ticked. Enter your WMS Pro login credentials in the Login and password field and enter the domain of the WMS Pro server (including the https prefix) to proceed.



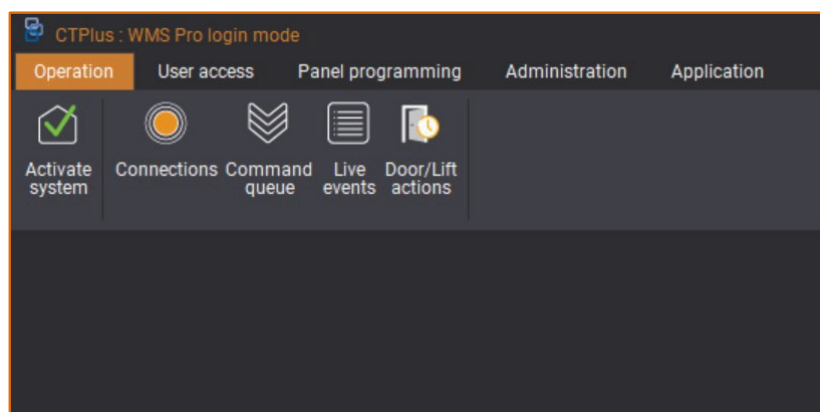
The WMS Pro domain is still the same as the one used for the WMS Pro installation. Any changes made in CTPlus while connected to WMS Pro will automatically save the changes to both WMS Pro and the selected Controller.

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: WMS Pro login mode:

- Panel programming is immediately loaded and available to the installer
- Changes made are saved immediately in WMS Pro and the hardware

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 list that appears. To use the CTPlus database, logout and then untick the **“WMS Pro login”** checkbox in the login page before logging back in.

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 one of 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
- If the card data belongs to a Credential group which is assigned to only one Controller, a mismatch is NOT 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.

Warning: Comms service not running

First time using WMS Pro? Click here to view quick start guide.

Controllers	Region : All Regions	Doors	Region : All Regions	Areas	Region : All Regions	Input testing	Region : All Regions
Online	0	2	Doors unlocked	3	Disarmed areas	5	Failed inputs
Total	4						

Recent history

Creation time	Device time	Device type	Event description
22/10/2024 05:19:27 AM		Operator	Operator admin, admin - Login
22/10/2024 05:18:31 AM	22/10/2024 05:18:31 AM	Automation zone	228 site C11 228 - auto tz 6 temp Off
22/10/2024 05:18:11 AM	22/10/2024 05:18:07 AM	Automation zone	228 site C11 228 - auto tz 6 temp On level 40%
22/10/2024 05:16:12 AM	22/10/2024 05:16:08 AM	Relay	228 site C11 228 - CH 1 Relay 96 Normal
22/10/2024 05:16:12 AM	22/10/2024 05:16:08 AM	Lift floor	228 site C11 228 - StandardLift 12 Floor 7 Auto secured
22/10/2024 05:16:12 AM	22/10/2024 05:16:08 AM	Area	228 site C11 228 - Area 5 Garage Out of timezone
22/10/2024 05:07:32 AM	22/10/2024 05:07:31 AM	Automation zone	228 site C11 228 - auto tz 6 temp Off
22/10/2024 05:07:12 AM	22/10/2024 05:07:07 AM	Automation zone	228 site C11 228 - auto tz 6 temp On level 40%
22/10/2024 05:00:12 AM	22/10/2024 05:00:12 AM	Standard door	228 site C11 228 - DWI Std Door 33 Unsecure

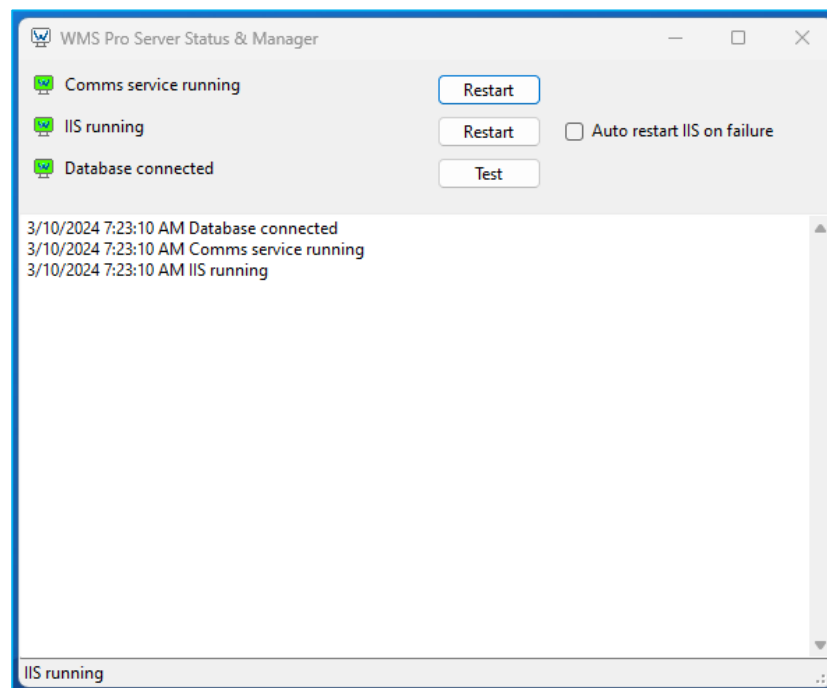
WMS Pro 2.2.76768 | API: v13.1.0 | Client: v13.1.0 [20241021]

If this occurs, it is recommended to open the “Services” Windows application on the WMS Pro server and search for “WMS Pro Comms Service” in the list, right-click on the name and select “Restart”. Once the service has been restarted, the error message should no longer appear and WMS Pro should be usable again.

UNRESPONSIVE PANELS

In WMS Pro, you may encounter an issue where WMS Pro cannot communicate with the 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 service using the WMS Pro Service Status & Manager app.



When using a unique instance name instead of SQL Express or the default SQL server instance "MSSQLSERVER", this may also affect communications between WMS Pro and Controllers. Please contact your system integrator or local TECOM distributor for further assistance with this issue.

WMS Pro Security Solutions

