



VIDEO WALL VIDEO PROCESSORS MULTIVIEWERS
DIGITAL SIGNAGE EXTENDERS CONTROL
CENTERS SCALERS WIRELESS



Professional Video Wall Controller & Management System



USER GUIDE V3.0

© 2026 Avenview Inc. All rights reserved.

The contents of this document are provided in connection with Avenview Inc. ("Avenview") products. Avenview makes no representations or warranties with respect to the accuracy or completeness of the contents of this publication and reserves the right to make changes to specifications and product descriptions at any time without notice. No license, whether express, implied, or otherwise, to any intellectual property rights is granted by this publication. Except as set forth in Avenview Standard Terms and Conditions of Sale, Avenview assumes no liability whatsoever, and disclaims any express or implied warranty, relating to its products of Avenview Inc. is strictly prohibited.

TABLE OF CONTENTS

1. PREREQUISITES	3
2. INTRODUCTION	3
3. MAIN FEATURES	3
4. OVERVIEW	4
5. SOFTWARE LICENSING OPTIONS	5
6. HARDWARE OPTIONS	6
6.1 AVXWALLPRO EMBEDDED (MICRO)	6
6.2 AVXWALLPRO COMPACT	7
6.3 AVXWALLPRO PROFESSIONAL	7
6.4 AVXWALLPRO SERVER (2U)	8
7. SYSTEM SETUP	9
7.1 WALL CONFIGURATION	10
7.2 COMMANDS	11
7.3 CONSOLE	11
7.4 SYSTEM MONITORING	12
7.5 NETWORK	12
7.6 DISPLAY	15
7.7 IDENTIFYING VIDEO OUTPUTS	15
7.8 MANAGING UHD DAISY-CHAIN DISPLAYS	16
7.9 ADVANCED SETTINGS	18
7.10 ADVANCED SETTINGS – USERS	18
7.11 ADVANCED SETTINGS – GROUPS	19
7.12 ADVANCED SETTINGS – CONFIG	20
8. INTEGRATION API	21
8.1 SERVICE AUTHENTICATION	21
8.2 SENDING COMMANDS	22
8.3 EXAMPLE RUNNING A SINGLE COMMAND	22
8.4 EXAMPLE RUNNING MULTIPLE COMMANDS	22
8.5 COMMAND LIST	23
9. AVXWALLPRO CONNECT	23
9.1 VNC	24
9.2 RDP	25

I. PREREQUISITES



Minimum configuration for the user interface in desktops:

- ⊕ PC with Intel® Core i3 Processor
- ⊕ Minimum of 4GB RAM
- ⊕ Operating systems: Windows, Linux or MacOS
- ⊕ Web browsers: Chrome, Firefox, Safari or Edge



The Screen Capture feature is compatible only with Google Chrome web browser and requires the installation of an Extension available at Google Play

Minimum configuration for the user interface in mobile devices:

- ⊕ Tablets or phones running Android 5.0 or Apple iOS 9

2. INTRODUCTION

The Avenview AVXWALLPRO™ is a lightweight, multi-platform solution for professional video walls, integrating all visual resources into a single canvas. It allows for smooth content handling to support decision-making and collaboration between local and remote peers in Command and Control Centers, War Rooms, and Digital Signage deployments.

Daily operations in Control Centers involve an intense volume of data that must be analyzed, monitored, and shared by teams. The AVXWALLPRO provides a powerful infrastructure, flexible enough to support operators in solving complex problems by aggregating IP streams, physical inputs, and web data onto a unified digital surface.

This manual presents hardware and software details to assist system administrators and users in configuring and operating the AVXWALLPRO system to extract maximum performance.

3. MAIN FEATURES

INTEGRATION

- iOS & Android Device Compatibility
- Integrated Videoconferencing (Zoom, Teams, Cisco, Skype, etc.)
- Media Server for Videos, Images & PDFs
- Audio Server Integration with Amplifiers
- GIS Mapping with Local Rendering
- Multi-User Mouse Control
- Industry-Leading VMS Integration
- HDMI Input Support
- Content Carousels for Dynamic Display
- Third-Party API Integration

INTERFACE

- Rich Dashboard with Intuitive GUI
- Drag-and-Drop Controls
- Web-Based Interface
- On-Screen Context Menu
- Integrated Web Browser
- Screen & Application Sharing
- Unified Workspace for Entire Video Wall
- Flexible Layout Management
- Built-in Support Apps (Clock, Weather, etc.)
- Desktop Workspace Splitter

NETWORK

- Virtual Desktop Infrastructure (VDI) Integration
- Remote Desktop Protocol (RDP) Support
- Distributed or Centralized Hardware Architecture
- Real-Time Video Streaming (HLS/RTSP/RTP)
- Remote Workstation Control (VNC)

SECURITY

- Robust Linux-Based Architecture
- Encrypted Authentication Certificates
- Advanced User & Group Management (LDAP)

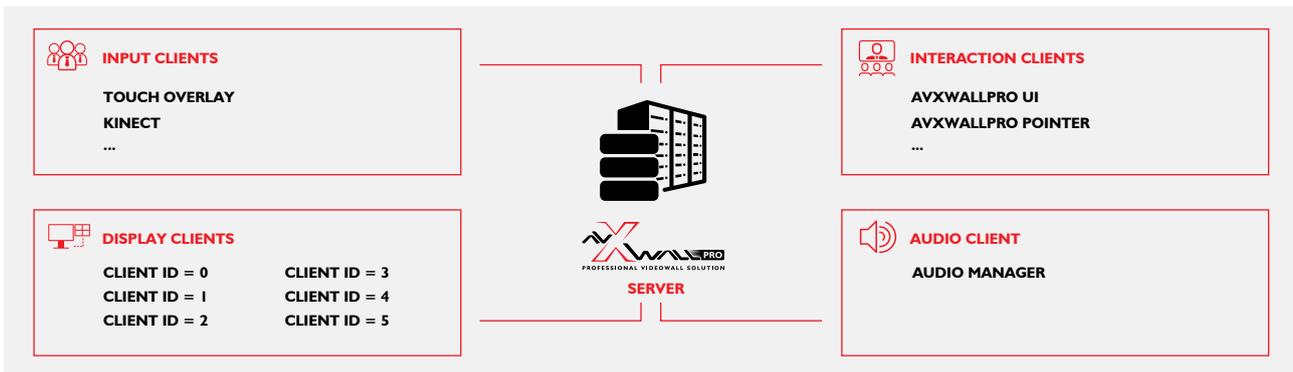
4. OVERVIEW

The Avenview AVXWALLPRO™ is a high-performance video wall controller ideal for small and large video wall in Control Rooms, Collaboration Rooms and Corporate Signage. Easily control and distribute all content sources to any display on your network with the utmost flexibility and full-featured management software.

The system presents itself as a computing appliance, usually known as Wall Controller. It is a computing device which provides predefined graphic and network services, and that has its underlying operating system hidden beneath an application-specific interface.

To improve performance and offer reduced complexity (e.g., installation, administration, and maintenance) and quicker deployment, the appliance hides the operating software and embeds the application within the device. It is based on a proprietary operating system, the AVXWALLPRO OS (Linux based).

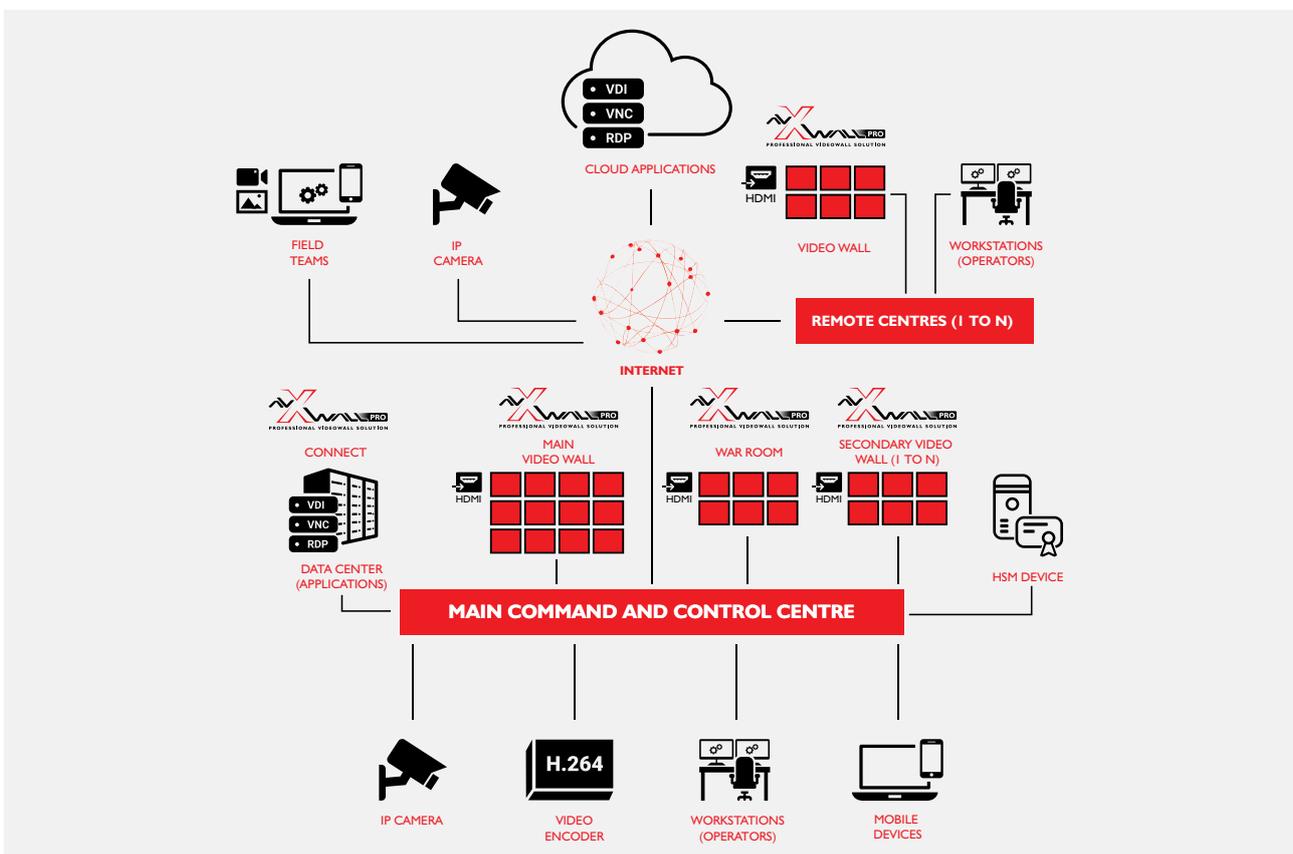
It consists of an appliance which can be installed in conjunction with a single display or a video wall (image manager – centralized system) or on a physical machine separated and connected via the Gigabit network to embedded computers installed on one or more video wall monitors (distributed system).



Users access the interaction Clients through a regular web browser, either from a computer desktop or from a mobile device. It is also possible to integrate touch panels, cameras, and videoconferencing systems. The audio of the video wall panel content can be connected to a central audio system or distributed by environments.

Sources from the network or from physical devices can be integrated to the AVXWALLPRO Control server for local displaying. Remote AVXWALLPRO servers from secondary rooms can

SYSTEM TOPOLOGY



5. SOFTWARE LICENSING OPTIONS



The AVXWALLPRO Control software is presented in three versions: Light, Standard and Full. Please check below the feature availability on each version:

	Light	Standard	Full	Meeting
Operation				
Web UI for operation	★	★	★	
Chrome extension for operation				★
Sign-in by token				★
Operation panel for tablet				★
Configuration				
Web UI for configuration	★	★	★	★
User and group management		★	★	
LDAP support			★	
Google Calendar Integration				★
Feature				
PDF presentation	★	★	★	★
On-screen Context Menu	★	★	★	★
REST API for integration	★	★	★	★
Screenshare	★	★	★	★
Smart Pointer	★	★	★	★
Layout management	★	★	★	
Layout scheduler	★	★	★	
Media Server for Video and Images	★	★	★	
Screenshot	★	★	★	
Offline layout management			★	
Automatic window arrangement				★
Hot stand-by			★	
Applications				
Clock	★	★	★	★
Web Browser	★	★	★	★
Facebook's Workplace	★	★	★	★
Google Maps	★	★	★	★
Google Meet	★	★	★	★
Microsoft Teams web	★	★	★	★
Skype web	★	★	★	★
Whereby	★	★	★	★
Whiteboard	★	★	★	★
Zoom web	★	★	★	★
HDMI input		★	★	★
Citrix Receiver		★	★	
RDP		★	★	
Vmware Esxi		★	★	
VNC		★	★	
RTSP/RTP video decoding			★	
Dashboard / Webpage Carrousel				★

6. HARDWARE OPTIONS

The AVXWALLPRO Control product line is composed by four distinct categories based on computational power, chassis form factor, and license options.

The categories are: Embedded, Compact, Professional and Server.

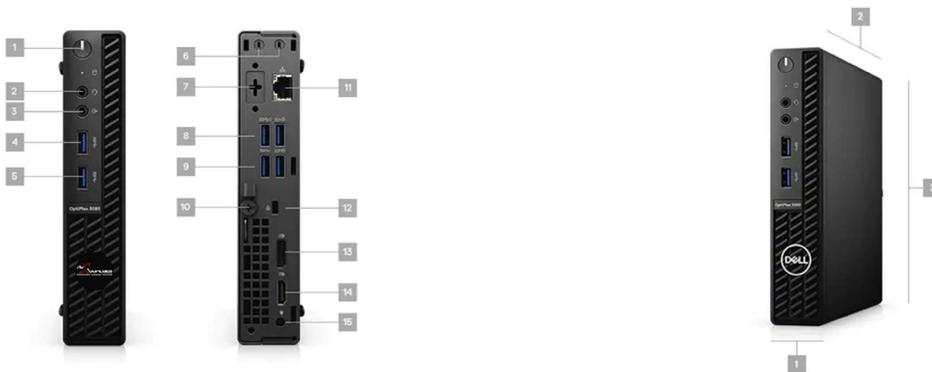
Find on the table below the main characteristics of each model:

FORM FACTOR	4K OUTPUTS	1080P INPUTS	4K INPUTS	SOFTWARE	
Embedded Micro	2	2	Custom	Basic	
Compact Tower	4	4	Custom	Advanced	
Professional Tower	8	8	Custom	Enterprise	
Server Rack 2U	16	Custom	Custom	Enterprise / Custom	

You must inform on your purchase order the desired video input max resolution, 4K or FHD. Mixing is not possible on the regular line, so contact your sales representative for custom configurations.

6.1 AVXWALLPRO EMBEDDED (MICRO)

Processor	Intel® Core™ i3-9100T (4 Cores, 4 Threads, 6MB Cache, 3.1GHz, 3.7GHz Turbo)
Memory	8GB 2666MHz DDR4 Memory
Storage	M.2 28GB Class 35 Solid State Drive
Video Output	Integrated Intel HD Graphics
Network	Wi-Fi Dual-band 2x2 802.11ac Wireless and 1 Gbps Ethernet Interface



Ports & Slots

1. Power Button | 2. Universal Audio Jack | 3. Line-out | 4. USB 3.2 Gen I Type-A port | 5. USB 3.2 Gen I Type-A port | 6. Knock-out Slots for Wireless Antenna | 7. Optional Video Port: Serial/DP 1.4/HDMI 2.0b/VGA | 8. USB 2.0 Ports (2) (1 with Smart Power on) | 9. USB 3.2 Gen I Type-A ports (rear) (2) | 10. Thumbscrew | 11. RJ-45 port 10/100/1000 Mbps | 12. K-lock Slot | 13. DisplayPort | 14. HDMI Port | 15. Power Connection

Dimensions & Weight

1. Width 1.4" (36 mm)
 2. Depth 7.0" (178 mm)
 3. Height 7.2" (183 mm)
Starting Weight 2.56 lb (1.16 kg)

6.2 AVXWALLPRO COMPACT

Processor	Intel Core i7-8700 (6 Cores, 12 Threads, 12MB Cache, 3.2GHz, 4.6GHz Turbo)
Memory	16GB 2666MHz DDR4 Memory
Storage	2.5" 256GB SATA Solid State Drive (SSD)
Video Output	1x NVIDIA Quadro P1000 (4GB GDDR5, 4 mini-DisplayPort 1.4)
Network	1 Gbps Ethernet Interface



Ports & Slots

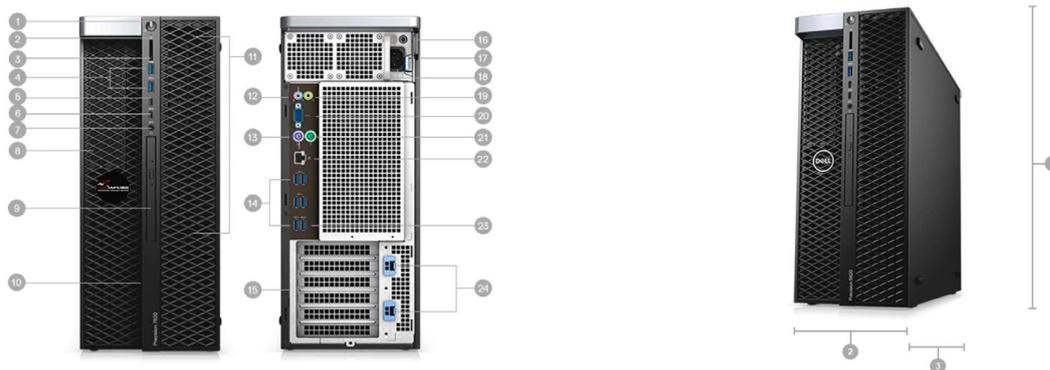
1. Power button | 2. Universal Audio Jack | 3. USB 3.2, Type A (Gen 2, 10Gbps) | 4. USB 3.2, Type A (Gen 2, 10Gbps) | 5. Optical Drive (optional) | 6. SD Card reader (optional) | 7. USB 3.2, Type C [10Gb] | 8. USB 3.2, Type A [5Gb] (Power share) | 9. Display Port 1.4 (2) | 10. PS2 Keyboard | 11. PS2 Mouse | 12. USB 2.0 Type A | 13. USB 3.2, Type A Gen 2 10Gbps (2 on left) Gen 1 5Gbps (2 on right) | 14. Audio Jack | 15. Lock slot | 16. RJ45 Network Connection | 17. Power Connection

Dimensions & Weight

1. Height: 13.19" (335mm)
 2. Width: 6.95" (176.6mm)
 3. Depth: 13.58" (345mm)
Weight: 23.37lb (10.60 kg)

6.3 AVXWALLPRO PROFESSIONAL

Processor	Intel Core i9-10900X (10 Cores, 20 threads, 19.25MB Cache, 3.7GHz, 4.5GHz Turbo)
Memory	16GB 2666MHz DDR4 Memory
Storage	2.5" 256GB SATA Solid State Drive (SSD)
Video Output	2x NVIDIA Quadro P2200 (5GB GDDR5X, 4 Display Port 1.4)
Network	1 Gbps Ethernet Interface



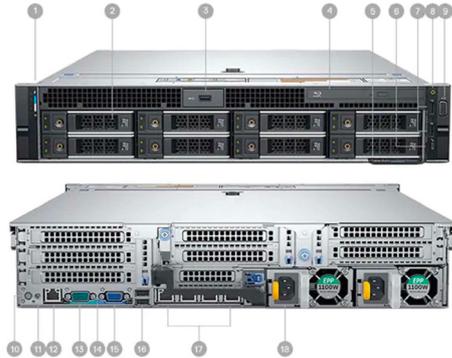
Ports & Slots

1. Power button/Power light | 2. Drive activity light | 3. SD card slot | 4. USB 3.1 Gen 1 ports | 5. USB 3.1 Gen 1 Type-C port with PowerShare | 6. USB 3.1 Gen 1 Type-C port | 7. Headset port | 8. 5.25 inch bay (optional) | 9. Optical drive | 10. Drive access release latch | 11. Drive carriers | 12. Microphone/Line-in port | 13. PS/2 Mouse port | 14. USB 3.1 Gen 1 ports | 15. Discrete graphics card slot (optional) | 16. Padlock ring | 17. Security cable slot | 18. Power cable connector | 19. Line-out port | 20. Serial port | 21. PS/2 Keyboard port | 22. Network port | 23. USB 3.1 Gen 1 port (supports smart Power-On) | 24. Expansion card slots

Dimensions & Weight

1. Height: 16.45" (417.9 mm)
 2. Width: 6.94" (176.5 mm)
 3. Depth: 20.4" (518.3 mm)
Starting weight: 32 lb (15.9kg)

Processor	Dual Intel Xeon Silver 4210 (10Cores, 20Threads, 13,75MBCache,2.2GHz,3.2GHz Turbo)
Memory	32GB 2666MHz DDR4 Memory
Storage	2.5" 256GB SATA Solid State Drive (SSD) – Raid available
Video Output	NVIDIA series
Network	4x 1 Gbps Ethernet Interface



Ports & Slots

1. System Status Indicator | 2. Hard drive (x8) | 3. USB 3.2 connector | 4. Optical-drive (optional) | 5. Information tag | 6. USB management port/iDRAC Direct | 7. USB 2.0 connector (x2) | 8. Power button/Power light | 9. VGA connector | 10. System identification button | 11. System identification connector | 12. iDRAC9 Enterprise Network connector | 13. Serial connector | 14. PCIe expansion card slots (x8) | 15. VGA connector | 16. USB 3.2 connectors (x2) | 17. Network connectors (x4) | 18. Power supply (x2)

Dimensions & Weight

1. Width: 18.98" (482 mm)
 2. Height: 3.42" (86.8 mm)
 3. Depth: 28.17" (715.5 mm)
Weight: 63.05 lb (28.6 kg)*

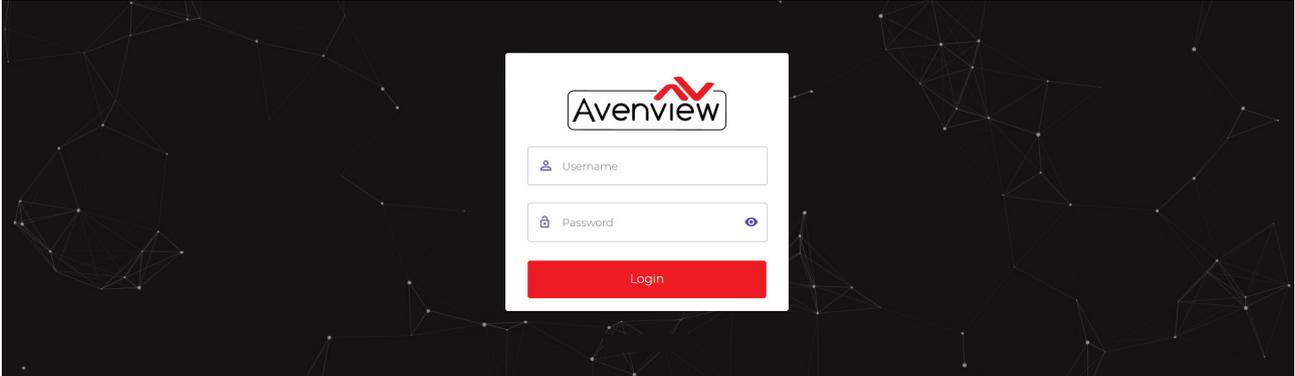


7. SYSTEM SETUP

The Administration Portal is the page that enables system administrators to change the video wall configuration, setup the hardware and modify some operating system parameters. Since AVXWALLPRO Control is an appliance, no access to the underlying operating system is possible: all configuration must be performed through the Administration Portal.

To get into the Administration Portal you must access through a web browser the AVXWALLPRO Control's IP on the port 10000.

As an example, the picture below illustrates an access from Chrome web browser:



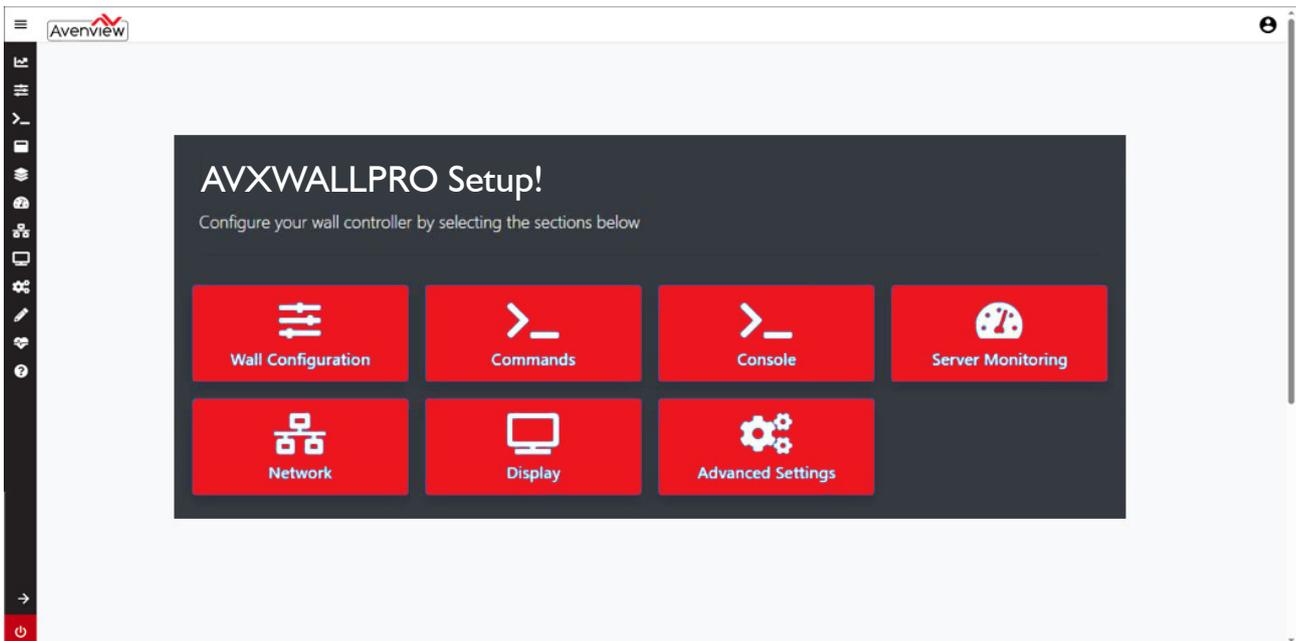
The syntax to be inserted in the URL web browser is `http://[server-ip]:10000`

As the Administration Portal shows up, the credentials must be inserted to login into the system.



The initial credentials are admin as username and admin as password. Please check how to change it in...

The Administration Portal Main Menu will be presented as the picture below:



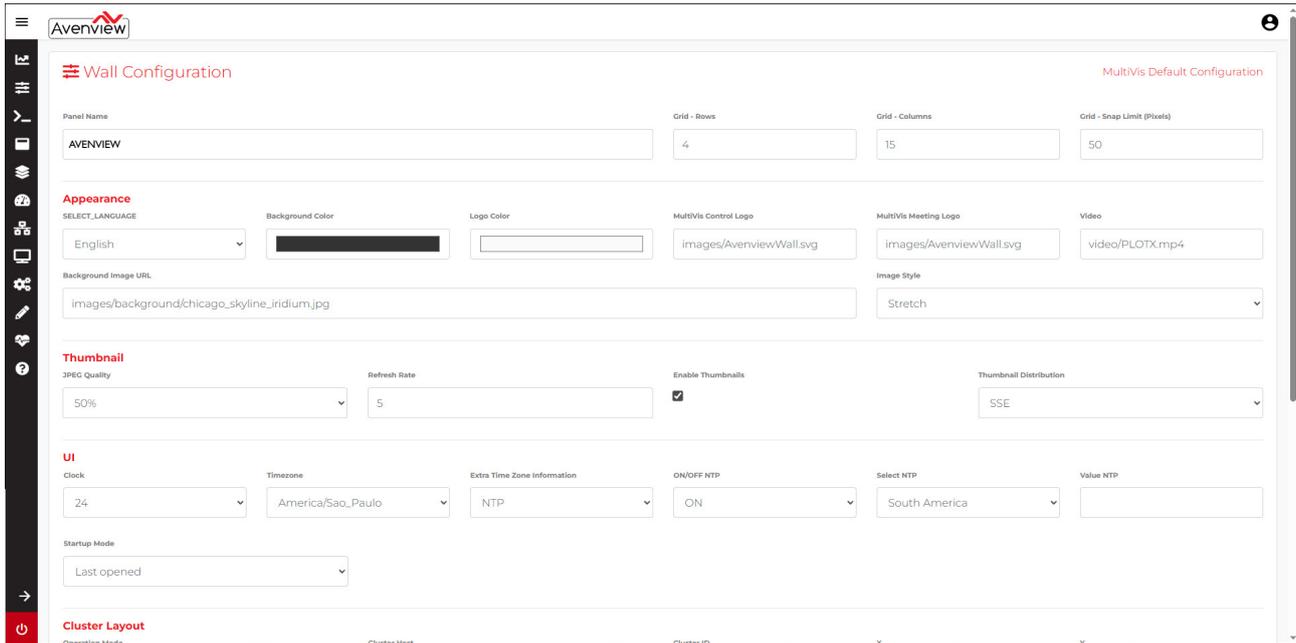
The AVXWALLPRO Control version is informed on the top of the main menu. Please use it when reporting problems.

There are seven different sessions as described below:

Wall configuration	To change appearance, UI grid, and set video wall canvas resolution
Commands	To execute commands on a low level
Console	To execute commands to the server through the API (expert)
System monitoring	To show the system health and status in real-time
Network	To change network parameters
Display	To configure the video driver
Advanced settings	For user management and hot stand-by configurations

7.1 WALL CONFIGURATION

On this session the administrator sets up the overall appearance of the video wall and some items of the operation user interface.

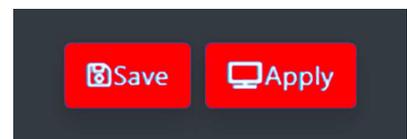


Each function is detailed on the table below:

Panel Name	A name can be set to the Video Wall Panel. It can be used to identify the room or the environment.
Grid – Rows	This configuration is related to the grid lines shown in the operation interface.
Grid – Columns	This configuration is related to the grid lines columns in the operation interface.
Grid – Snap Limit (Pixels)	Sets the sensibility of the “Snap to the grid” function. The default value is 50.
Background color	Sets the background color of the video wall canvas.
Logo color	Sets the logo color shown at the video wall canvas.
AVXWALLPRO Control logo	Path to the AVXWALLPRO Control logo image file.
AVXWALLPRO Meeting logo	Path to the AVXWALLPRO Meeting logo image file.
Video	Path to the video background shown at the video wall canvas.
Initial volume	Initial audio volume. (1-100)
Clock	Option to 12- or 24-hours clock.
Width	The width in pixels of the video wall canvas.
Height	The height in pixels of the video wall canvas.
Cluster Layout	Rows and Columns must be set to 1 (do not change).
Alternate hosts	If needed, additional alternate host can be informed.
Remote Sites	Not in use.

Please be aware that after the modification of any value you must press the button ‘Save’. The “Apply” button can be pressed if the user wants to change the configuration immediately. The Save and Apply buttons are located at the bottom of the page.

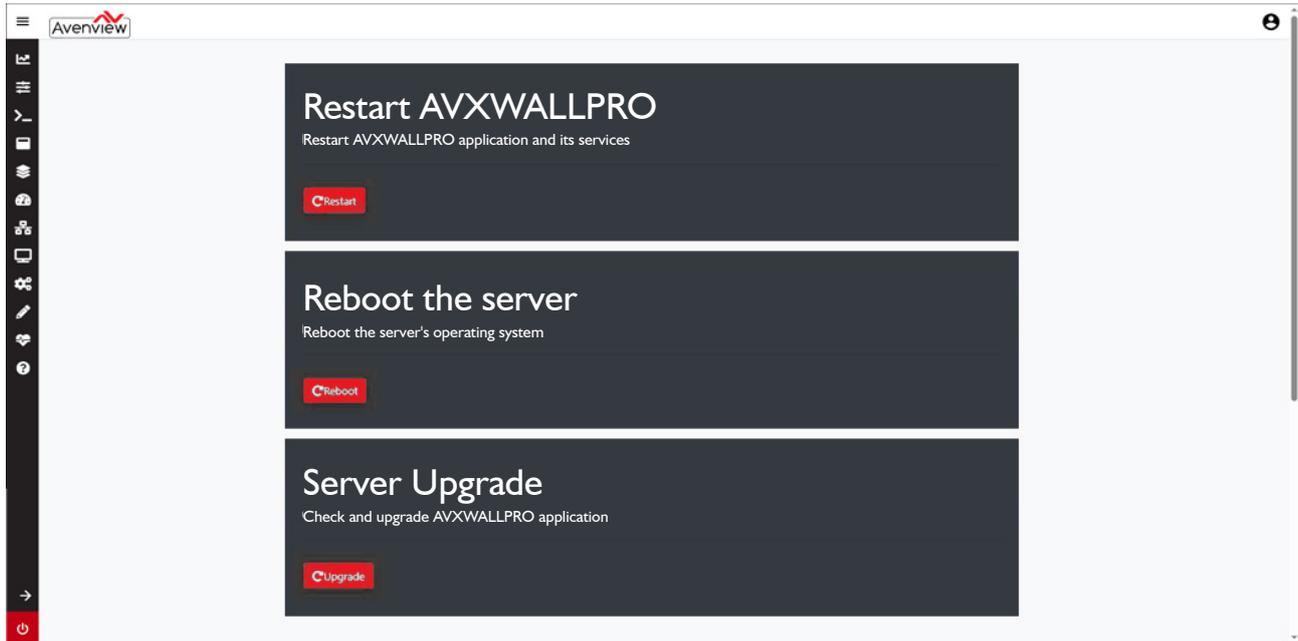
If you cannot apply the changes, the system restart can be performed when suitable on the session ‘Commands’, detailed on the next page.



When the ‘Apply’ button is used, the video wall canvas will restart, blink, and go back to the initial status. So be cautious to not using it during Control Room operation.

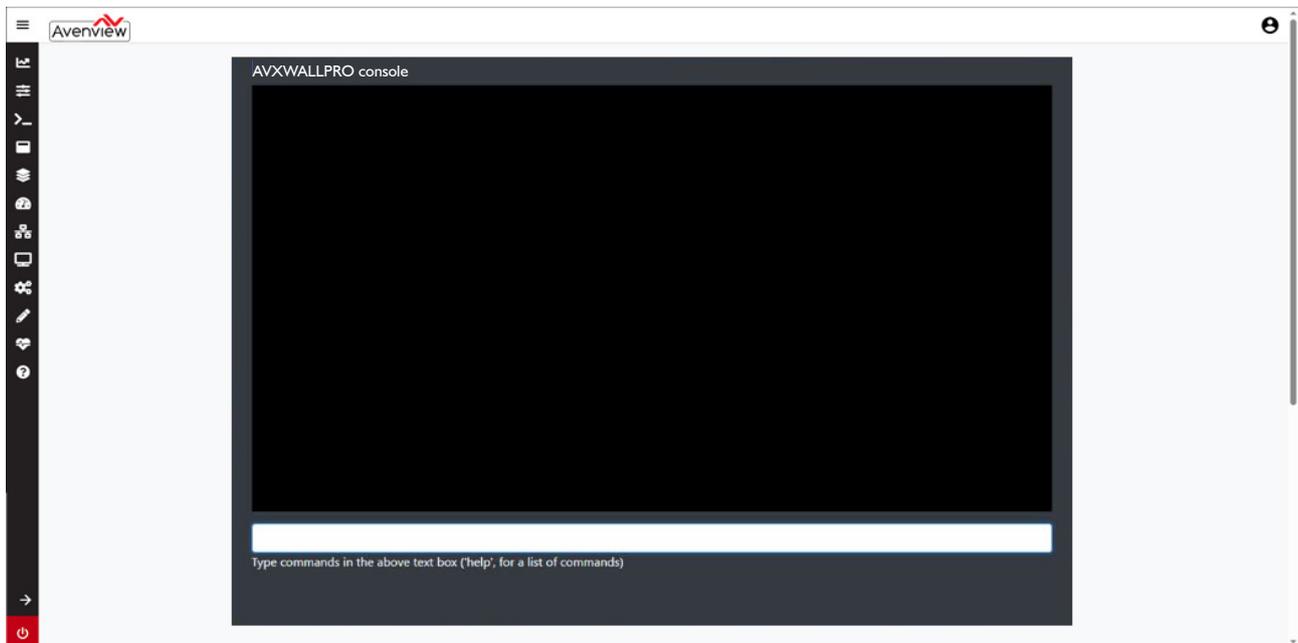
7.2 COMMANDS

On this session the administrator sets up the overall appearance of the video wall and some items of the operation user interface.



Restart AVXWALLPRO	This command will restart all software services related to the AVXWALLPRO Control. When applied, the video wall canvas will restart, blink, and go back to the initial status.
Reboot the server	This command will restart the computer itself, at the level of the operating system.
Server upgrade	This command will check the AVXWALLPRO repositories and suggest software updates, if available.

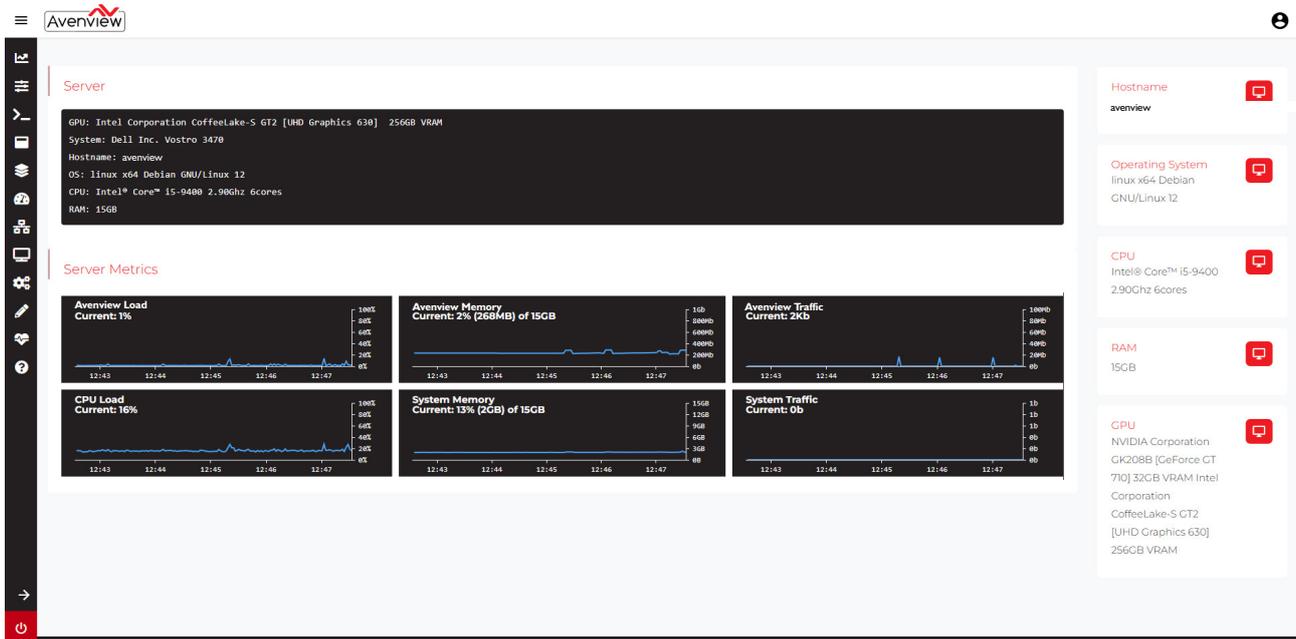
7.3 CONSOLE



This page is intended for expert users and for maintenance. It will send direct commands to the server through the software API. The commands will not be detailed on this manual.

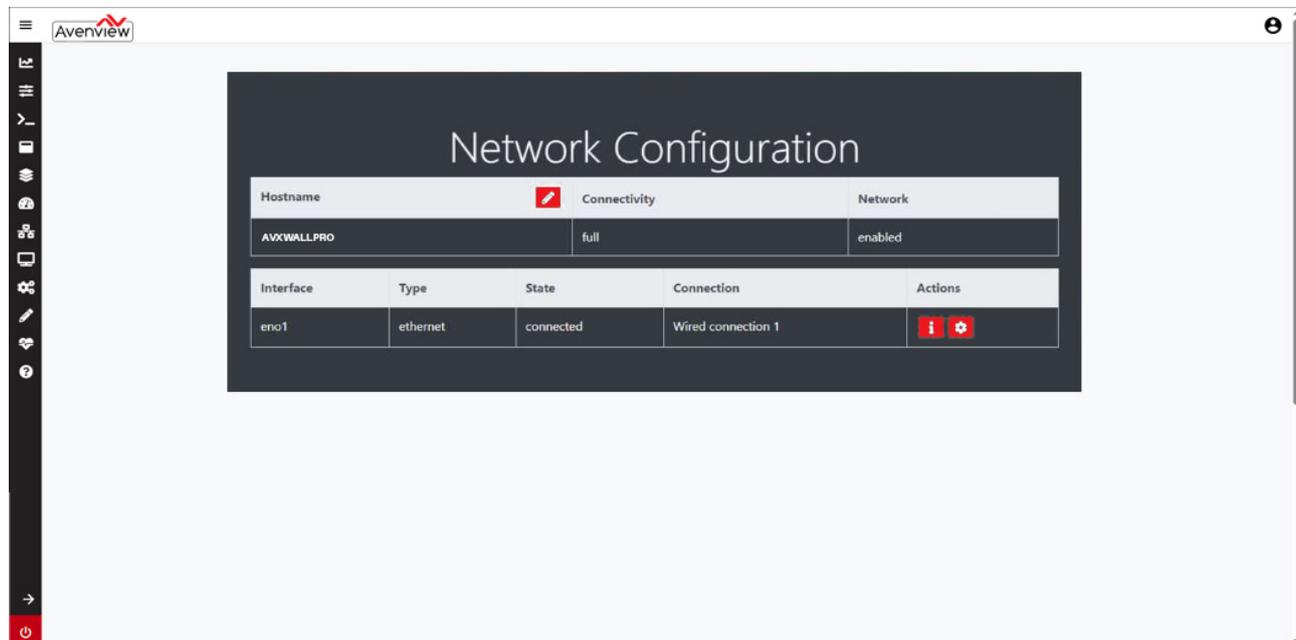
7.4 SYSTEM MONITORING

Allows system administrators to check in real-time the computer specification, the load of AVXWALLPRO Control threads, the load on CPU and memory, and the traffic at the network interface.



7.5 NETWORK

This session allows system administrators to configure all network interfaces of the computer. The initial setup of AVXWALLPRO Control controllers are automatic IP addressing by DHCP on the 'eno1' ethernet interface (wired connection).

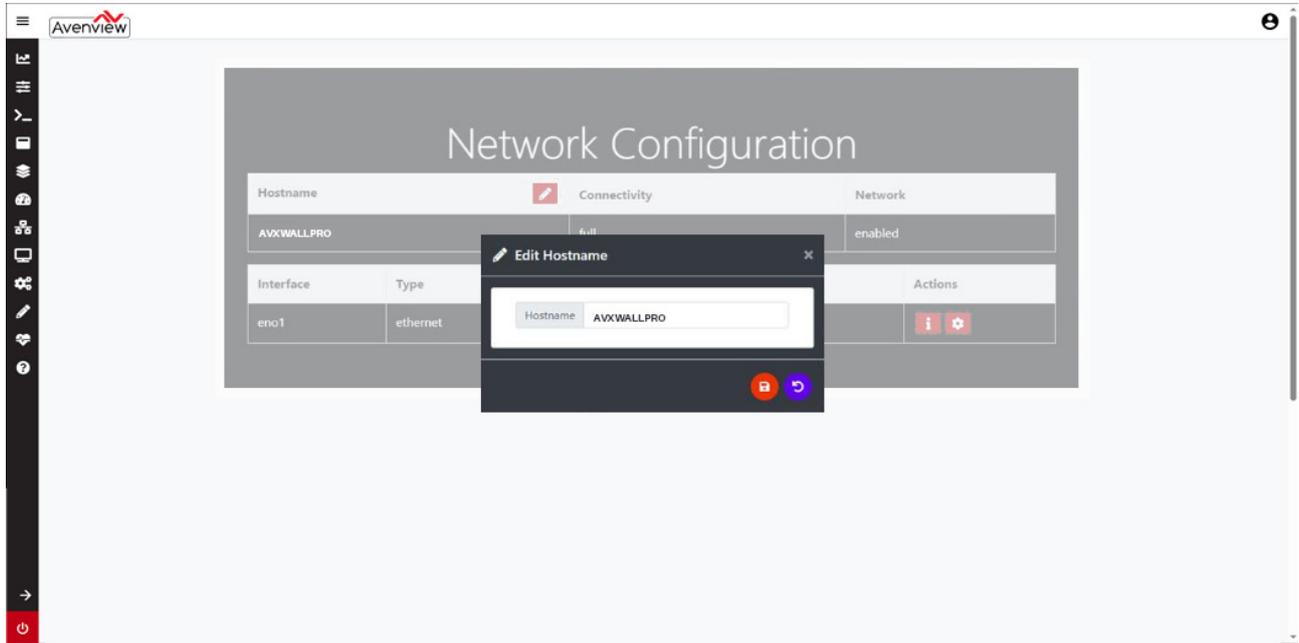


When using this session, press the red button to save and the violet button to retrieve the previous value.

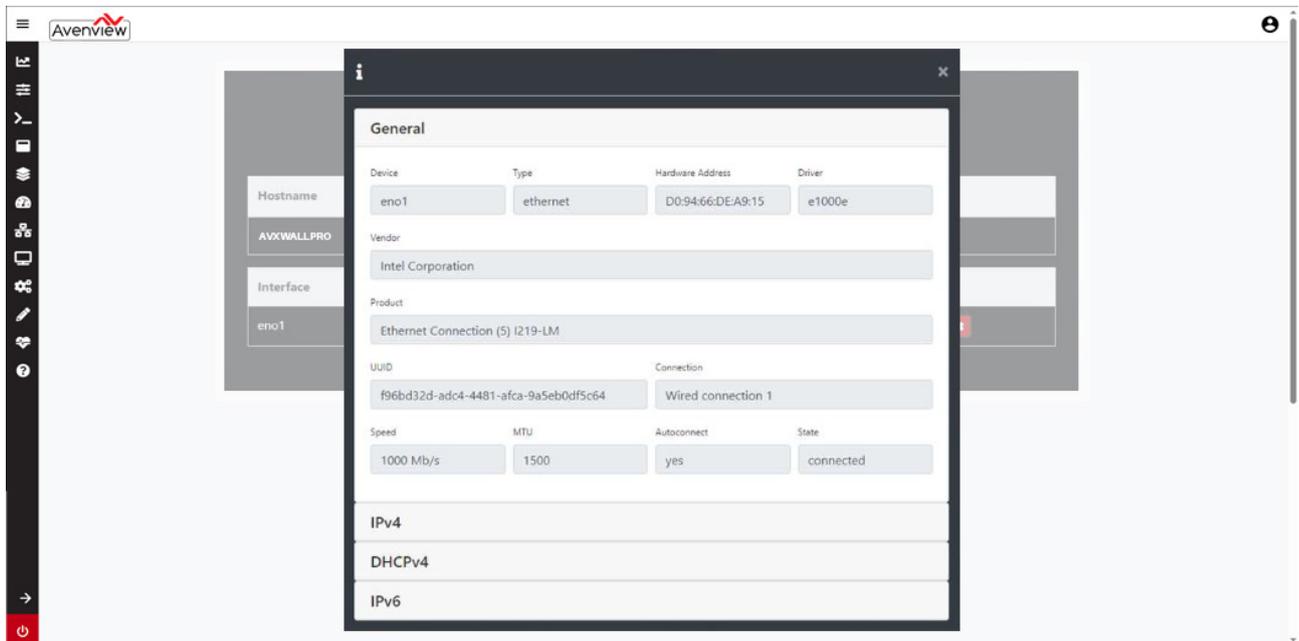


At this page, administrators can set a new hostname by pressing the button 

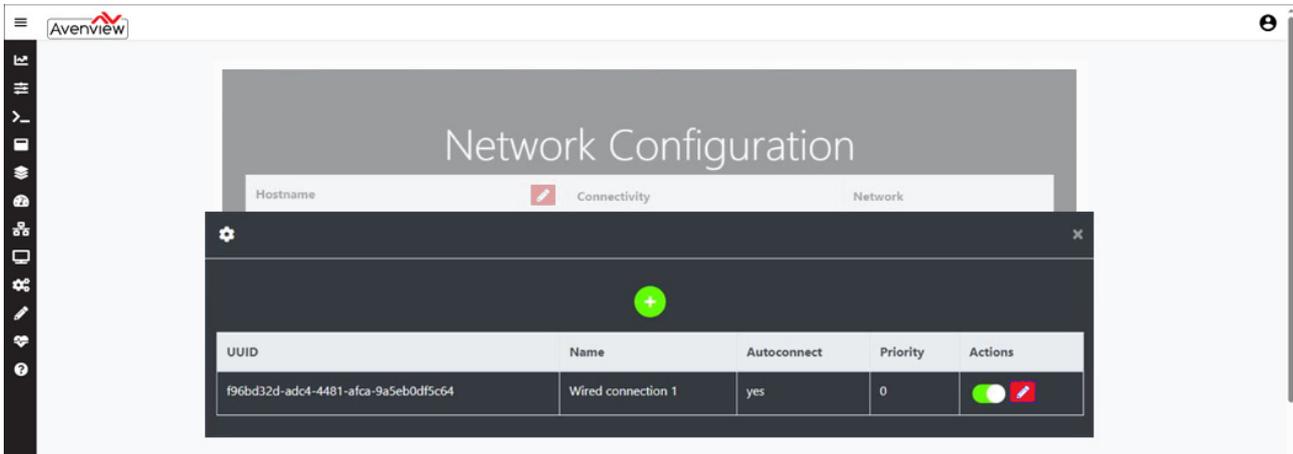
The dialog box below appears, and the new name can be set.



By pressing the button,  the details of the interface and the connection will be displayed. On this dialog box, the system administrator can check the General settings, the IPv4 details, the DHCP v4 details and the IPv6 details.



By pressing the button,  will be granted to the administrator the function, to change the interface and connection details. The following screen will show up:

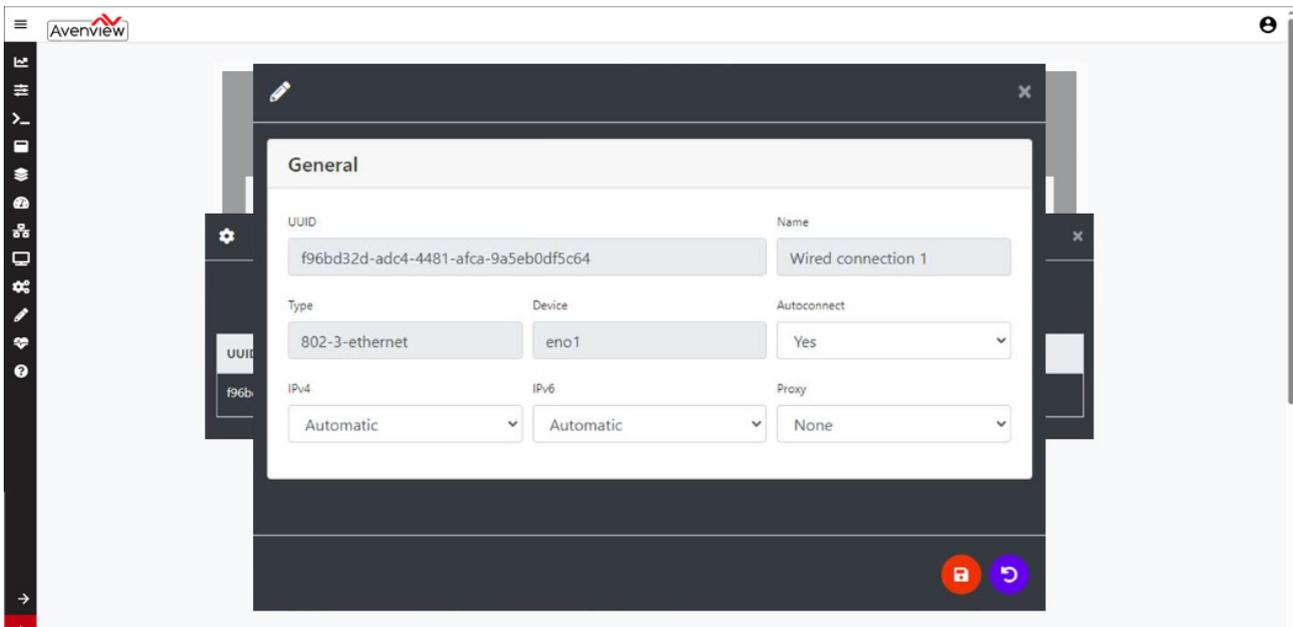


The button  is inserted on the computer. is used to add a new network interface. It must be used only when a new interface

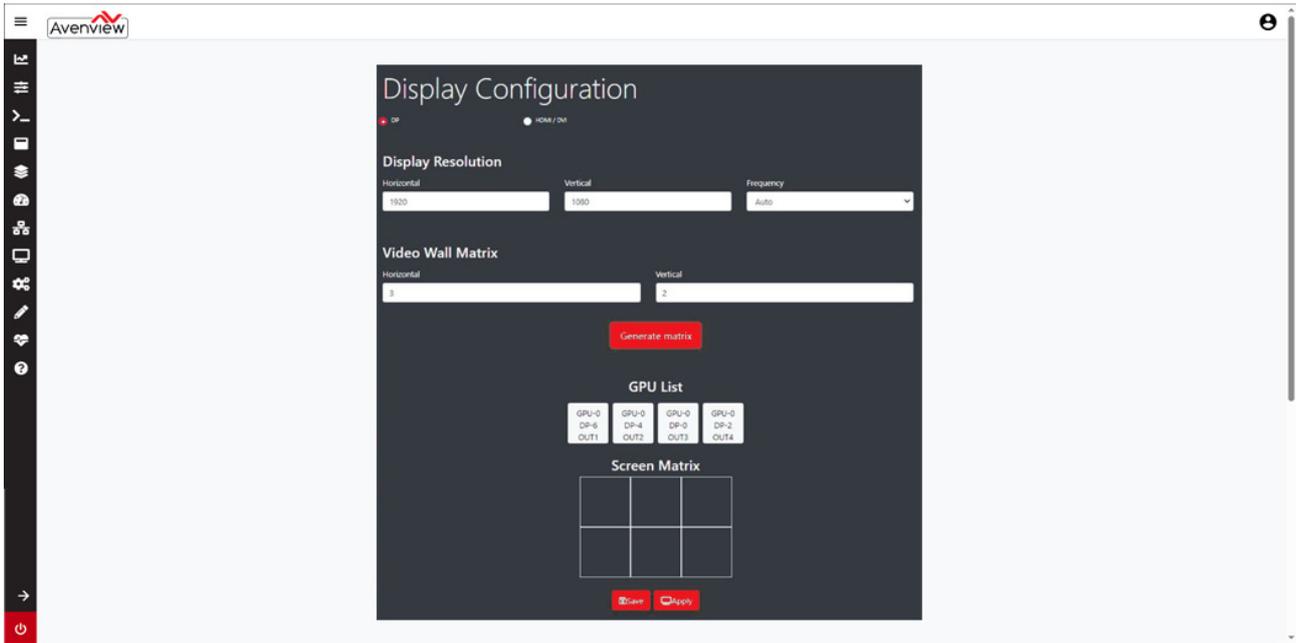
 Don't try to insert a new interface if no new network card was inserted.

The button  enables or disables the selected interface.

By pressing the  button, system administrator can change the following configurations:



Autoconnect	Connects to the network automatically. Available options: Yes / No
IPv4	Available options: - Disabled - Automatic: means DHCP on - Manual: allows the configuration of the IP address, the gateway, the DNS, and Search Domains
IPv6	Available options: - Disabled - Automatic: means DHCP on - Manual: allows the configuration of the IP address, the gateway, the DNS, and Search Domains
Proxy	Available options: - None - Automatic: Browser only (yes/no) and PAC URL (to set the URL to the automatic configuration script)



This session allows system administrators to change the video driver parameters. AVXWALLPRO Control Embedded series comes with an Intel HD Graphics GPU. Compact, Professional and Server categories are powered by NVIDIA QUADRO cards.

The steps to create a new display configuration are the following:

1. First, you must select the video interface type you're using at the display. You can select either DP for Display Port or HDMI/DVI.
2. Then, inform the display resolution details: Type the width in pixels (e.g. 1920), the height in pixels (e.g. 1080) and select the display's refresh rate (30 Hz, 60 Hz or Automatic). If you don't know the refresh rate, please set the Automatic option.
3. Now inform the video wall formation, i.e., the count of displays you have on the horizontal axis by the count of displays you're using on the vertical axis.
4. Press the button Generate matrix and the representation of your video wall will be displayed with the controller's GPU outputs list.
5. Drag each GPU output (the white squares) to the position the display is connected in your video wall. To identify the video outputs and set advanced matrix configurations refer to the next session, Managing video outputs.
6. Press the Save button and then the Apply button. The video wall canvas will blink, but the content will remain.



The refresh rate is determined by the display and cables together. So, if you know that your display supports 60Hz but it's displaying only 30 Hz, please check the cables specs and the cable/connector condition.



Be sure that the video wall width and height set on the Wall configuration session is the same as configured on this one.

7.7 **IDENTIFYING VIDEO OUTPUTS**

There are cases that some advanced configurations must be performed to configure the video outputs and achieve the video wall requirements. As an example, there are video walls formed by Full HD displays with the UHD daisy-chain feature, which drives up to four FHD displays from a single 4K output.

First, it is important to explain how to identify the video outputs on the wall controller.

On systems equipped with Nvidia Quadro P1000 cards:

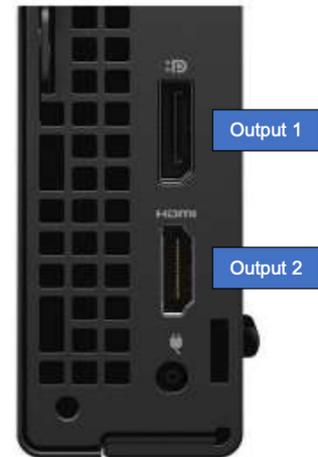


On systems equipped with Nvidia Quadro P2200 cards:

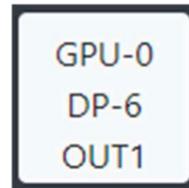


As the Nvidia output's nomenclature is quite odd, please refer to the reference table below to identify the right correlation:

OUTPUT #	DP	HDMI
Output 1	DP-6	DP-7
Output 2	DP-4	DP-5
Output 3	DP-0	DP-1
Output 4	DP-2	DP-3



The maximum number of Nvidia GPUs on a single system will be four. They will be identified as GPU-0, GPU-1, GPU-2, and GPU-3. So, the first output of the first GPU will be represented as follows:



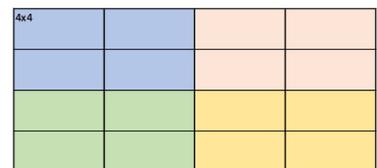
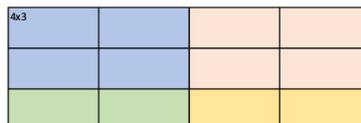
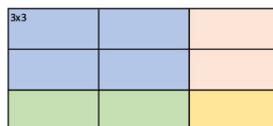
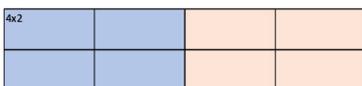
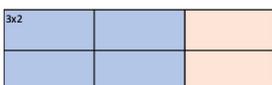
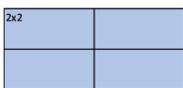
For the embedded systems equipped with Intel graphic cards, the physical outputs will be:

7.8 MANAGING UHD DAISY-CHAIN DISPLAYS

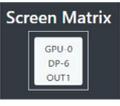
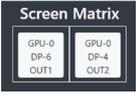
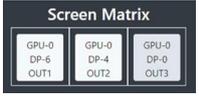
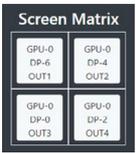
The UHD daisy-chain is a feature present in many displays nowadays. This function allows the distribution of a single 4K signal (3840x2160 pixels) up to four FHD displays (1920x1080 pixels).

The following diagrams illustrates the possible video wall formations when using displays with UHD daisy-chain and a wall controller with a single 4-outputs Nvidia card. Each 2x2 display set requires one DP cable from the wall controller and three cables to the internal display loop.

Label:



One may deduce that with just a single 4-outputs card it's possible to drive up to 16 FHD displays. At the table below some video wall formation examples are shown with its detailed parameters to be set in the Display session:

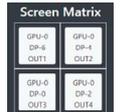
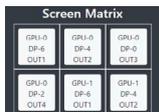
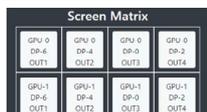
VW form	Display Resolution H	Display Resolution V	Refresh rate	Video Wall Matrix H	Video Wall Matrix V	Matrix
2x2	3840	2160	Auto, 30Hz or 60Hz	1	1	
3x2 4x2				2	1	
5x2 6x2				3	1	
7x2 8x2				4	1	
3x3 4x3 4x4				4	1	

The same logic must be applied for wall controllers with more than one video card, but it's out of the scope of this manual. In case of doubts, please contact our support team at support@avenview.com e-mail address.



The output order in the display shown at the table above is just a suggestion. You can set the displays the way you want.

For cases where no UHD-loop is possible, the display setup becomes straightforward. The table below shows the same video wall formations of the first table, but with different parameters. In this case one may need up to four video cards on a single system to get the same video wall formation.

VW form	Display Resolution H	Display Resolution V	Refresh rate	Video Wall Matrix H	Video Wall Matrix V	Matrix
2x2	The display horizontal resolution (e.g. 1920, 3840, etc.)	The display horizontal resolution (e.g. 1080, 2160, etc.)	Auto, 30Hz or 60Hz	2	2	
3x2				3	2	
4x2				4	2	

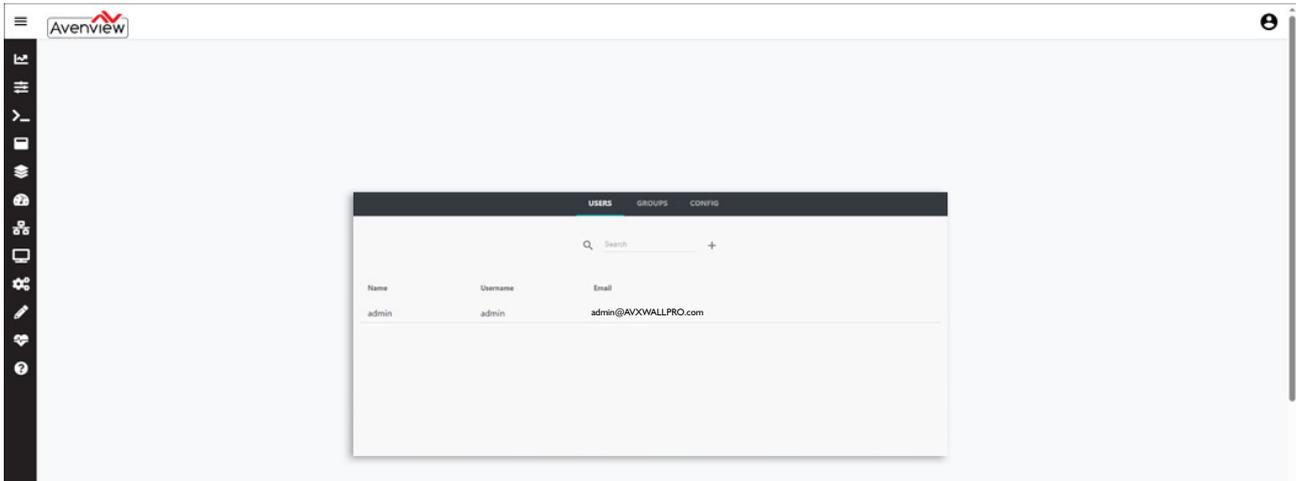
And so on for 5x2, 6x2, 7x2, 8x2, 3x3, 4x3, and 4x4 formations.



AVXWALLPRO Control versions powered by Nvidia cards can display up to 5120x2880@60Hz. The ones equipped with Intel HD Graphics the maximum resolution will be 3840x2160@60Hz.

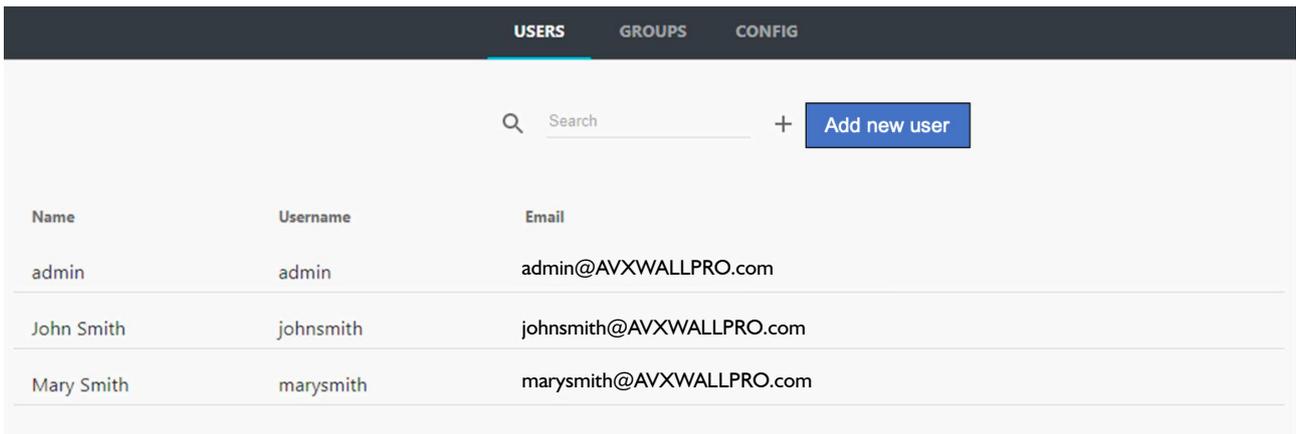
7.9 ADVANCED SETTINGS

On this session are presented settings for user and group management and an advance setup for the hot stand-by option. The picture below shows the session main page, where the user can select the options Users, Groups and Config. On the next pages we will show each one of them.

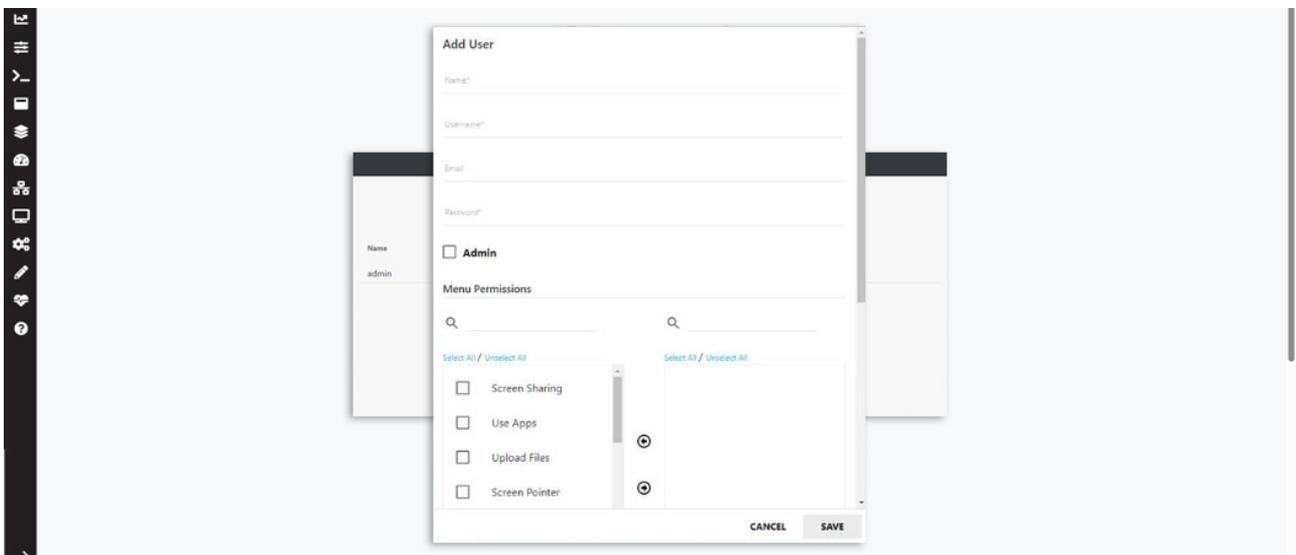


7.10 ADVANCED SETTINGS – USERS

On this option the administrators can search, create, edit, and delete users who will have access to the operation and administration interfaces.



To add a new user, press the '+' button besides the search dialog box. The following modal screen will be displayed:



You must inform the identification of the user, as his full name, username and password. You can also inform his e-mail address, but it's optional.

The **Admin** checkbox sets administrator privileges to the user, i.e. provides access to the administration portal. Users with this role can change any system parameter, so be cautious.

Administrators can also modify the user's **Menu Permissions**. On the picture below, the left column shows all available menu items. At the right column, the menu items allowed to the user.

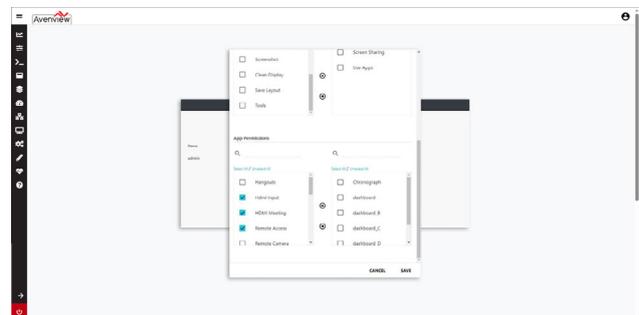
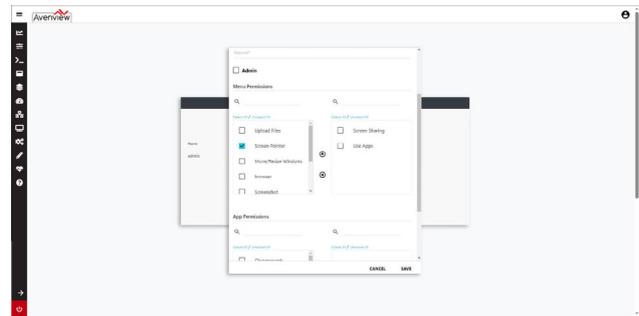
To allow the menu item to appear on the user interface, one may select the checkbox of the selected item on the left column and press the button ► (arrow to right).

To not allow the menu item to appear on the user interface, one may select the checkbox of the item on the right column and press the button ◀ (arrow to left).

To change the **App Permissions**, proceed the same way as with the Menu permissions.

To allow the application to appear on the user interface, one may select the checkbox of the selected item on the left column and press the button ► (arrow to right).

To not allow the application to appear on the user interface, one may select the checkbox of the item on the right column and press the button ◀ (arrow to left).



Press **Save** to write the changes and close the modal or **Cancel** to abandon the changes.

7.11

ADVANCED SETTINGS – GROUPS

On this option the administrators can search, create, edit, and delete **groups of users**, allowing the attribution of **Menu and App Permissions** to more than one user at once.

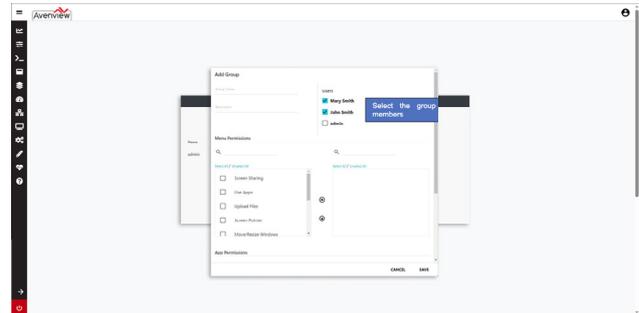
USERS GROUPS CONFIG	
<input type="text" value="Search"/> + Add new group	
Group Name	Description
Administrators	System administrators group
Operators	Control room operator's group

To add a new group, press the '+' button besides the search dialog box. The following modal screen will be displayed:

Inform the **Group Name** and the group's **Description** on the fields at the top left. Using the checkboxes on the top right, select the users who will be assigned to this group.

Configure the **Menu** and **App permissions** as explained on the section before, Advanced settings.

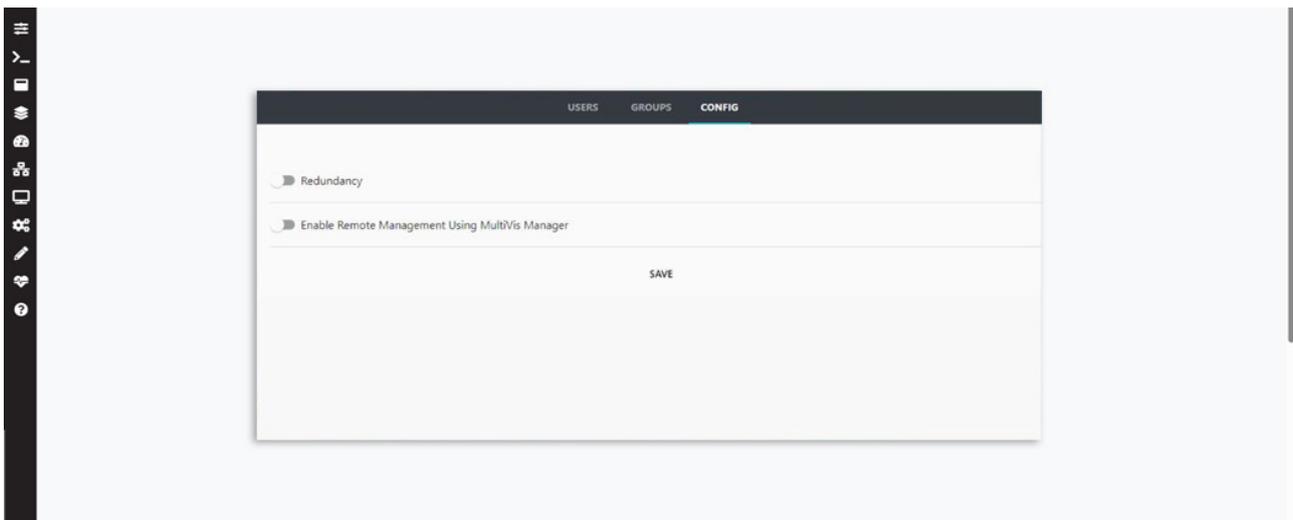
Press **Save** to write the changes and close the modal or **Cancel** to abandon the changes.



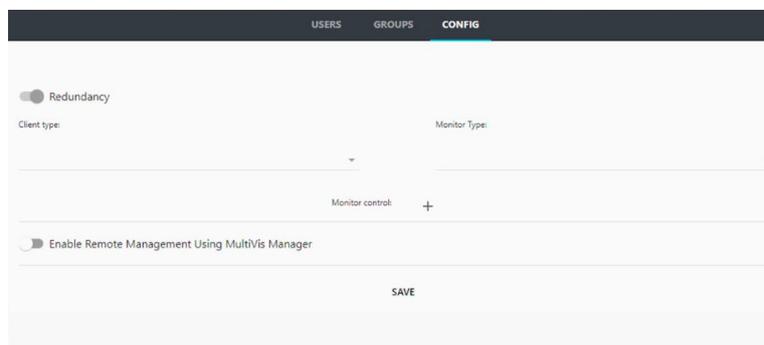
7.12 ADVANCED SETTINGS – CONFIG

This session allows system administrators to configure the Hot stand-by setting on the **Redudancy** option shown on the picture below.

The option **Enable Remote Management Using AVXWALLPRO Manager** is no longer in use and will be removed on the next update.



By pressing on the **Redudancy** button, the following screen will be presented:



Client type	Select if the wall controller is the Master or the Slave
Monitor type	Select the displays brand: Delta, Samsung, or LG

After the setup of the parameters above, press the '+' button at the right side of Monitor control. It will create a command line for each display at the video wall,

Command type	Specify if the wall controller is connected to the displays through a serial cable or through the network. Options: IP/Serial
Switching input type	Select the desired video input to switch
Monitor ID	The display address
Monitor IP	The display IP address, when needed

8. INTEGRATION API

On this session the steps to establish a communication between AVXWALLPRO Control and an external system using the Postman app.

<https://www.postman.com/downloads/>

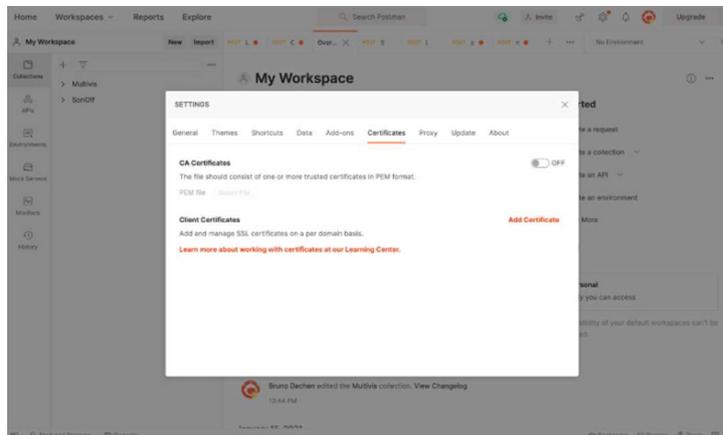


This session is intended to expert users, with experience in REST API communications and web services.

8.1 SERVICE AUTHENTICATION

Since it's a secure channel, the first action is to authenticate and get the token from the server. Follow the steps below:

Step 1: Remove Postman CA Certificates



Step 2: Set the Header Flag Content-type to "application/json"

Step 3: Send a request to the server 'https://serverIP:3000/login' including in the request body the username and the password: the default is admin/admin.



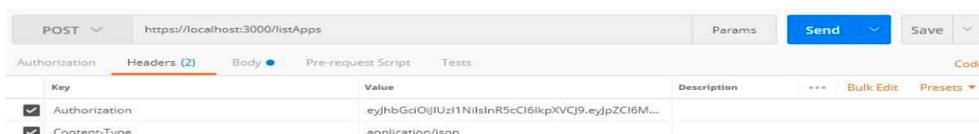
Step 4: Response: from the response copy the token flag. This will be used to authenticate all the commands send to the AVXWALLPRO system.

```

1 <
2 {"token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9
3 .eyJpZiI6Im50ZW50aW50IiwiaWF0IjoiMjAxNy00LTI1
4 Wl0iLCJ0eXBlIjoiYm9keSIsImVhbnQI6Ij0iLCJ1aW50
5 LmVhbnQI6Ij0iLCJ1aW50LmVhbnQI6Ij0iLCJ1aW50
6 LmVhbnQI6Ij0iLCJ1aW50LmVhbnQI6Ij0iLCJ1aW50
7 LmVhbnQI6Ij0iLCJ1aW50LmVhbnQI6Ij0iLCJ1aW50
8 LmVhbnQI6Ij0iLCJ1aW50LmVhbnQI6Ij0iLCJ1aW50
9 LmVhbnQI6Ij0iLCJ1aW50LmVhbnQI6Ij0iLCJ1aW50
10 LmVhbnQI6Ij0iLCJ1aW50LmVhbnQI6Ij0iLCJ1aW50
11 LmVhbnQI6Ij0iLCJ1aW50LmVhbnQI6Ij0iLCJ1aW50
12 LmVhbnQI6Ij0iLCJ1aW50LmVhbnQI6Ij0iLCJ1aW50
  
```

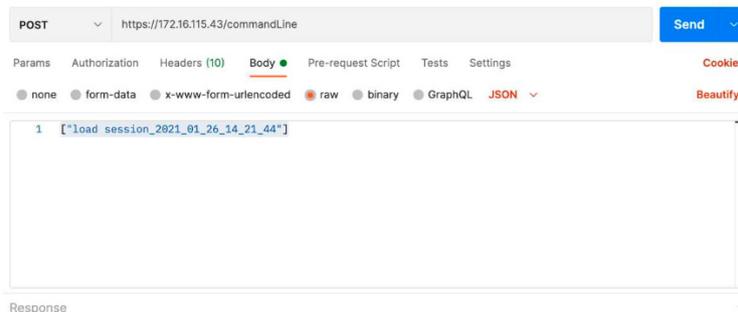
8.2 SENDING COMMANDS

From the authentication response, take the Token and add the Authorization header flag to the POST command:



All commands must be sent to the service **'https://serverIP/commandLine'** by POST in the request body, on a JSON format in a String Array. The Token generated in the first step and the Content-Type "application/json" must be informed in the request header.

8.3 EXAMPLE RUNNING A SINGLE COMMAND



8.4 EXAMPLE RUNNING MULTIPLE COMMANDS



Command	Function	Syntax	Parameters
assets	Lists the existing applications	["assets"	N/A
clear	Close all running applications	["clear"]	N/A
fullscreen	Maximize an application	["fullscreen app_id"]	app_id: the application ID
hardware	Lists the server hardware resources	["hardware"]	N/A
hide UI	Hide/show the UI upper bar	["hideui"]	N/A
kill	Close an application	["kill app_id"]	app_id: the application ID
load	Call a preset layout	["load layout"]	layout: the desired layout ID
session	Lists existing layouts IDs and names	['sessions']	N/A
move by	Shifts a window	["moveby app_id dx dy"]	app_id: the application ID dx: desired shift on x-axis in pixels dy: desired shift on y-axis in pixels
move to	Moves a window to a specific position	["moveto app_id x y"]	app_id: the application ID x: desired coordinate for the application on the x-axis, in pixels y: desired coordinate for the application on the y-axis, in pixels
resize	Resize a window	["resize app_id width height"]	app_id: the application ID width: desired width in pixels height: desired height in pixels
save	Saves the current layout	["save name"]	name: name for the file creation
screenshot	Takes a screen shot of the wall	['screenshot']	N/A
bring to front	Places the application in front of all others	["brintofront app_id"]	app_id: the application ID
send to back	Places the application behind all others	["sendtoback app_id"]	app_id: the application ID

9. AVXWALLPRO CONNECT

AVXWALLPRO Connect is a gateway that integrates RDP and VNC sessions to AVXWALLPRO Control. In this chapter, you'll learn how to access its setup portal and create new connections.

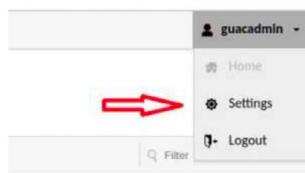
Using a regular web browser, you can access the AVXWALLPRO connect server by the following URL:

http://[AVXWALLPRO_CONTROL_IP]:8081/connect/

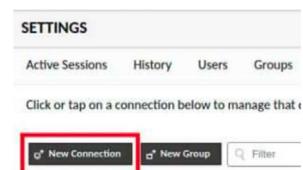
On the first access, use the following credentials:

USERNAME: admin
PASSWORD: admin

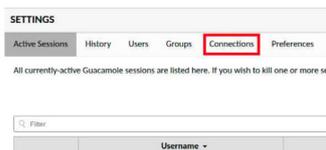
On this page, click on the drop-down menu located on the right top corner of the page and select the item 'Settings'.



Press the button 'New connection':



Then click on connections and on the new screen press the button 'New connection'.



The page below will be presented, allowing the parametrization of the remote connections:



To set a remote connection on AVXWALLPRO, the following fields must be configured. Each protocol supported by AVXWALLPRO Connect has its own set of configuration parameters. These parameters typically describe the hostname and port of the remote desktop server, the credentials to use when connecting, if any, and the size and color depth of the display. If the protocol supports file transfer, options for enabling that functionality will be provided as well.

'EDIT CONNECTION' session

NAME: insert a name for the connection

PROTOCOL: Choose between RDP and VNC

The VNC protocol is the simplest and first protocol supported by AVXWALLPRO Connect. Although generally not as fast as RDP, many VNC servers are adequate, and VNC over AVXWALLPRO Connect tends to be faster than VNC by itself due to decreased bandwidth usage.

Network parameters

Except for the reverse-mode VNC connections, VNC works by making outbound network connections to a particular host that runs one or more VNC servers. Each VNC server is associated with a display number, from which the appropriate port number is derived.

Hostname

The hostname or IP address of the VNC server AVXWALLPRO Connect should connect to.

Port

The port the VNC server is listening on, usually 5900 or 5900 + display number. For example, if your VNC server is serving display number 1 (sometimes written as :1), your port number here would be 5901

Autoretry

The number of times to retry connecting before giving up and returning an error. In the case of a reverse connection, this is the number of times the connection process is allowed to time out.

Display settings

VNC servers do not allow the client to request particular display sizes, so you are at the mercy of your VNC server concerning display width and height. However, to reduce bandwidth usage, you may request that the VNC server reduce its color depth. AVXWALLPRO Connect will automatically detect 256-color images, but this can be guaranteed for absolutely all graphics sent over the connection by forcing the color depth to 8-bit. Color depth is otherwise dictated by the VNC server.

If you are noticing problems with your VNC display, such as the lack of a mouse cursor, the presence of multiple mouse cursors, or strange colors (such as blue colors appearing more like orange or red), these are typically the result of bugs or limitations within the VNC server, and additional parameters are available to work around such issues.

color-depth

The color depth to request, in bits-per-pixel. This parameter is optional. If specified, this must be either 8, 16, 24, or 32. Regardless of what value is chosen here, if a particular update uses less than 256 colors, AVXWALLPRO Connect will always send that update as a 256-color PNG.

swap-red-blue

If the colors of your display appear wrong (blues appear orange or red, etc.), it may be that your VNC server is sending image data incorrectly, and the red and blue components of each color are swapped. If this is the case, set this parameter to "true" to work around the problem. This parameter is optional.

cursor

If set to "remote", the mouse pointer will be rendered remotely, and the local position of the mouse pointer will be indicated by a small dot. A remote mouse cursor will feel slower than a local cursor but may be necessary if the VNC server does not support sending the cursor image to the client.

encodings

A space-delimited list of VNC encodings to use. The format of this parameter is dictated by libvncclient and thus doesn't follow the form of other AVXWALLPRO Connect parameters. This parameter is optional, and libguac-client-vnc will use any supported encoding by default.

Beware that this parameter is intended to be replaced with an individual encoding-specific parameters in a future release.

read-only

Whether this connection should be read-only. If set to "true", no input will be accepted on the connection at all. Users will only see the desktop and whatever other users using that same desktop are doing. This parameter is optional.

Authentication

The VNC standard defines only password-based authentication. Other authentication mechanisms exist but are non-standard or proprietary. AVXWALLPRO Connect supports only the password method.

Parameter name

Password

Description

The password to use when attempting authentication if any. This parameter is optional.

Which VNC server?

The choice of VNC server can make a big difference when it comes to performance, especially over slower networks. While many systems provide VNC access by default, using this is often not the fastest method.

RealVNC or TigerVNC

RealVNC, and its derivative TigerVNC, perform quite well. In our testing, they perform the best with AVXWALLPRO Connect. If you are okay with having a desktop that can only be accessed via VNC, one of these is likely your best choice. Both optimize window movement and (depending on the application) scrolling, giving a very responsive user experience.

TightVNC

TightVNC is widely-available and performs generally as well as RealVNC or TigerVNC. If you wish to use TightVNC with AVXWALLPRO Connect, performance should be just fine, but we highly recommend disabling its JPEG encoding. This is because images transmitted to AVXWALLPRO Connect are always encoded losslessly as PNG images. When this operation is performed on a JPEG image, the artifacts present from JPEG's lossy compression reduce the compressibility of the image for PNG, thus leading to a slower experience overall than if JPEG was simply not used, to begin with.

x11vnc

The main benefit of using x11vnc is that it allows you to continue using your desktop normally, while simultaneously exposing control of your desktop via VNC. The performance of x11vnc is comparable to RealVNC, TigerVNC, and TightVNC. If you need to use your desktop locally as well as via VNC, you will likely be quite happy with x11vnc.

Vino

vino is the VNC server that comes with the Gnome desktop environment and is enabled if you enable "desktop sharing" via the system preferences available within Gnome. If you need to share your local desktop, we recommend using x11vnc rather vino, as it has proven more performant and feature-complete in our testing. If you don't need to share a local desktop but simply need an environment you can access remotely, using a VNC server like RealVNC, TigerVNC, or TightVNC is a better choice.

QEMU or KVM

QEMU (and thus KVM) expose the displays of virtual machines using VNC. If you need to see the virtual monitor of your virtual machine, using this VNC connection is your only choice. As the VNC server built into QEMU cannot be aware of higher-level operations like window movement, resizing, or scrolling, those operations will tend to be sent suboptimally, and will not be as fast as a VNC server running within the virtual machine. If you wish to use a virtual machine for desktop access, we recommend installing a native VNC server inside the virtual machine after the virtual machine is set up. This will give a more responsive desktop.

9.2 RDP

The RDP protocol is more complicated than VNC. It tends to be faster than VNC due to the use of caching, which AVXWALLPRO Connect does take advantage of.

Network parameters

RDP connections require a hostname or IP address defining the destination machine. The RDP port is defined to be 3389 and will be this value in most cases. You only need to specify the RDP port if you are not using port 3389.

Hostname

The hostname or IP address of the RDP server AVXWALLPRO Connect should connect to.

Port

The port the RDP server is listening on, usually 3389. This parameter is optional. If this is not specified, the default of 3389 will be used.

Authentication and security

RDP provides authentication through the use of a username, password, and optional domain. Most RDP servers will provide a graphical login if the username, password, and domain parameters are omitted. One notable exception to this is Network Level Authentication, or NLA, which performs all authentication outside of a desktop session, and thus in the absence of a graphical interface. If your server requires NLA, you will need to manually choose this as your security mode, and you must provide a username and password. All RDP connections are encrypted. Higher-grade encryption is available in the form of TLS, another possible security mode.

Hostname

The username to use to authenticate, if any. This parameter is optional.

password

The password to use when attempting authentication, if any. This parameter is optional.

domain

The domain to use when attempting authentication, if any. This parameter is optional.

security

The security mode to use for the RDP connection. This mode dictates how data will be encrypted and what type of authentication will be performed if any. By default, standard RDP encryption is requested, as it is the most widely supported.

Possible values are:

rdp

Standard RDP encryption. This is the default and should be supported by all RDP servers.

nla

Network Level Authentication. This mode requires the username and password and performs an authentication step before the remote desktop session actually starts. If the username and password are not given, the connection cannot be made.

tls

TLS encryption. TLS (Transport Layer Security) is the successor of SSL.

any

Allow the server to choose the type of security.

ignore-cert

If set to "true", the certificate returned by the server will be ignored, even if that certificate cannot be validated. This is useful if you universally trust the server and your connection to the server, and you know that the server's certificate cannot be validated (for example, if it is self-signed).

disable-auth

If set to "true", authentication will be disabled. Note that this refers to authentication that takes place while connecting. Any authentication enforced by the server over the remote desktop session (such as a login dialog) will still take place. By default, authentication is enabled and only used when requested by the server. If you are using NLA, authentication must be enabled by definition.

Session settings

RDP sessions will typically involve the full desktop environment of a normal user. Alternatively, you can manually specify a program to use instead of the RDP server's default shell, or connect to the administrative console.

Although AVXWALLPRO Connect is independent of the keyboard layout, RDP is not. This is because AVXWALLPRO Connect represents keys based on what they do ("press the Enter key"), while RDP uses identifiers based on the key's location ("press the rightmost key in the second row"). To translate between a AVXWALLPRO Connect key event and an RDP key event, AVXWALLPRO Connect must know ahead of time the keyboard layout of the RDP server.

By default, the US English qwerty keyboard will be used. If this does not match the keyboard layout of your RDP server, keys will not be properly translated, and you will need to explicitly choose a different layout in your connection settings.

client-name

When connecting to the RDP server, AVXWALLPRO Connect will normally provide its hostname as the name of the client. If this parameter is specified, AVXWALLPRO Connect will use its value instead.

On Windows RDP servers, this value is exposed within the session as the CLIENTNAME environment variable.

console

If set to "true", you will be connected to the console (admin) session of the RDP server.

initial-program

The full path to the program to run immediately upon connecting. This parameter is optional.

server-layout

The server-side keyboard layout. This is the layout of the RDP server and has nothing to do with the keyboard layout in use on the client. The AVXWALLPRO Connect client is independent of the keyboard layout. The RDP protocol, however, is not independent of the keyboard layout, and AVXWALLPRO Connect needs to know the keyboard layout of the server to send the proper keys when a user is typing.

Possible values are:

en-us-qwerty - English (US) keyboard	(qwertz)	sv-se-qwerty - Swedish keyboard
en-gb-qwerty - English (UK) keyboard	it-it-qwerty - Italian keyboard	tr-tr-qwerty - Turkish-Q keyboard
de-de-qwertz - German keyboard (qwertz)	ja-jp-qwerty - Japanese keyboard	failsafe
fr-fr-azerty - French keyboard (azerty)	pt-br-qwerty - Portuguese Brazilian keyboard	
fr-ch-qwertz - Swiss-French keyboard	es-es-qwerty - Spanish keyboard	

Unknown keyboard – this option sends only Unicode events and should work for any keyboard, though not necessarily all RDP servers or applications. If your server’s keyboard layout is not yet supported, this option should work in the meantime.

Display settings

AVXWALLPRO Connect will automatically choose an appropriate display size for RDP connections based on the size of the browser window and the DPI of the device. The size of the display can be forced by specifying explicit width or height values.

To reduce bandwidth usage, you may also request that the server reduce its color depth. AVXWALLPRO Connect will automatically detect 256-color images, but this can be guaranteed for absolutely all graphics sent over the connection by forcing the color depth to 8-bit. Color depth is otherwise dictated by the RDP server.

color-depth

The color depth to request, in bits-per-pixel. This parameter is optional. If specified, this must be either 8, 16, or 24. Regardless of what value is chosen here, if a particular update uses less than 256 colors, AVXWALLPRO Connect will always send that update as a 256-color PNG.

width

The width of the display to request, in pixels. This parameter is optional. If this value is not specified, the width of the connecting client display will be used instead.

dpi

The desired effective resolution of the client display, in DPI. This parameter is optional. If this value is not specified, the resolution and size of the client display will be used together to determine, heuristically, an appropriate resolution for the RDP session.

resize-method

The method to use to update the RDP server when the width or height of the client display changes. This parameter is optional. If this value is not specified, no action will be taken when the client display changes size.

Normally, the display size of an RDP session is constant and can only be changed when initially connecting. As of RDP 8.1, the “Display Update” channel can be used to request that the server change the display size. For older RDP servers, the only option is to disconnect and reconnect with the new size.

Possible values are:

display-update

Uses the “Display Update” channel added with RDP 8.1 to signal the server when the client display size has changed.

reconnect

Automatically disconnects the RDP session when the client display size has changed and reconnects with the new size.

Performance flags

RDP provides several flags that control the availability of features that decrease performance and increase bandwidth for the sake of aesthetics, such as wallpaper, window theming, menu effects, and smooth fonts. These features are all disabled by default within AVXWALLPRO Connect such that bandwidth usage is minimized, but you can manually re-enable them on a per-connection basis if desired.

enable-wallpaper

If set to “true”, enables the rendering of the desktop wallpaper. By default, the wallpaper will be disabled, such that unnecessary bandwidth need not be spent redrawing the desktop.

enable-theming

If set to “true”, enables the use of theming of windows and controls. By default, theming within RDP sessions is disabled.

enable-font-smoothing

If set to "true", the text will be rendered with smooth edges. The text over RDP is rendered with rough edges by default, as this reduces the number of colors used by text, and thus reduces the bandwidth required for the connection.

enable-full-window-drag

If set to "true", the contents of windows will be displayed as windows are moved. By default, the RDP server will only draw the window border while windows are being dragged.

enable-desktop-composition

If set to "true", graphical effects such as transparent windows and shadows will be allowed. By default, such effects, if available, are disabled.

enable-menu-animations

If set to "true", menu open and close animations will be allowed. Menu animations are disabled by default.

disable-bitmap-caching

In certain situations, particularly with RDP server implementations with known bugs, it is necessary to disable RDP's built-in bitmap caching functionality. This parameter allows that to be controlled in a AVXWALLPRO Connect session. If set to "true" the RDP bitmap cache will not be used.

disable-offscreen-caching

RDP normally maintains caches of regions of the screen that are currently not visible in the client to accelerate retrieval of those regions when they come into view. This parameter, when set to "true," will disable caching of those regions. This is usually only useful when dealing with known bugs in RDP server implementations and should remain enabled in most circumstances.

disable-glyph-caching

In addition to screen regions, RDP maintains caches of frequently used symbols or fonts, collectively known as "glyphs." As with bitmap and offscreen caching, certain known bugs in RDP implementations can cause performance issues with this enabled, and setting this parameter to "true" will disable that glyph caching in the RDP session.

RemoteApp

Recent versions of Windows provide a feature called RemoteApp which allows individual applications to be used over RDP, without providing access to the full desktop environment. If your RDP server has this feature enabled and configured, you can configure AVXWALLPRO Connect connections to use those individual applications.

remote-app

Specifies RemoteApp to start on the remote desktop. If supported by your remote desktop server, this application, and only this application, will be visible to the user.

Windows requires a special notation for the names of remote applications. The names of remote applications must be prefixed with two vertical bars. For example, if you have created a remote application on your server for notepad.exe and have assigned it the name "notepad", you would set this parameter to: "Inotepad".

remote-app-dir

The working directory, if any, for the remote application. This parameter has no effect if RemoteApp is not in use.

remote-app-args

The command-line arguments, if any, for the remote application. This parameter has no effect if RemoteApp is not in use.

Avenview Warranty Certificate

AVENVIEW CORP. ("Avenview") warrants Avenview-branded product(s) contained in the original packaging against defects in materials and workmanship when used normally in accordance with Avenview's enclosed manual guidelines for a period of THREE (3) YEARS from the date of original retail purchase - Warranty Period. Avenview's published guidelines include but are not limited to information contained in technical specifications, user manuals and service communications.

LABOR: During the Warranty Period of THREE (3) YEARS, Avenview will repair or replace the product(s) at no cost using new or used parts equivalent to novel performance and reliability if the product(s) is determined to have abide by Avenview's published guidelines. Cost of Labor applicable to product(s) after Warranty Period. For labor costs, please contact support@avenview.com.

PARTS: During the Warranty Period of THREE (3) YEARS, Avenview will supply new or rebuilt replacements in exchange for defective parts of the product(s) at no cost if the product(s) is determined to have abide by Avenview's published guidelines. Cost of Parts applicable to product(s) after Warranty Period. For part(s) costs, please contact support@avenview.com.

To obtain Warranty: (a) proof of purchase in the form of a bill of sale or receipted invoice reflecting that the registered product(s) is within warranty period must be presented to obtain warranty service; (b) product(s) must be registered at time of purchase. Failure to do so will result in applicable parts and labor charges. Returning product(s) must be shipped in Avenview's original packaging or in packaging pertaining equal degree of protection to Avenview's. Both Avenview and purchaser are responsible for freight charges and brokerages when shipping the product(s) to the receiver.

NOT COVERED BY THIS WARRANTY

This warranty does not apply to any non-Avenview branded product(s); non-registered Avenview product(s). This warranty does not apply: (a) to cosmetic damage, including but not limited to scratches, dents and broken cords; (b) to damage caused by use with another product; (c) to damage caused by accident, abuse, misuse, liquid contact, fire, earthquake or other external cause; (d) to damage caused by operating the Avenview product(s) outside Avenview's manuals or guidelines; (e) to damage caused by service performed by anyone who is not a representative of Avenview or an Avenview authorized personnel; (f) to defects caused by normal wear and tear or otherwise due to the normal aging of the Avenview product(s), or (g) if any serial number has been removed or defaced from the Avenview product(s).

AVENVIEW IS NOT LIABLE FOR DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM ANY BREACH OF WARRANTY OR CONDITION, OR UNDER ANY OTHER LEGAL THEORY, INCLUDING BUT NOT LIMITED TO LOSS OF USE; LOSS OF REVENUE; LOSS OF ACTUAL OR ANTICIPATED PROFITS (INCLUDING LOSS OF PROFITS ON CONTRACTS); LOSS OF THE USE OF MONEY; LOSS OF ANTICIPATED SAVINGS; LOSS OF BUSINESS; LOSS OF OPPORTUNITY; LOSS OF GOODWILL; LOSS OF REPUTATION; LOSS OF, DAMAGE TO, COMPROMISE OR CORRUPTION OF DATA; OR ANY INDIRECT OR CONSEQUENTIAL LOSS OR DAMAGE REPAIR OR REPLACEMENT AS PROVIDED UNDER THIS WARRANTY IS THE EXCLUSIVE REMEDY OF THE CONSUMER.

Some states do not allow the inclusion or limitation of incidental or consequential damages, or allow limitations on duration implements of the Warranty Period; therefore the above limitations or exclusions may not be applicable to you. This warranty gives you specific legal rights, and you may have other rights which vary from state to state.



275 Woodward Avenue, Kenmore, NY 14217
1.866.508.0269



AVENVIEW CORP

+ 1 716 218 4100

sales@avenview.com

+ 1 866 387 8764

1100 Military Road Kenmore, NY | 4217

Disclaimer

The material in this manual is for informational purposes only. The products it describes are subject to change without prior notice due to the manufacturer's continuous development program. Avenview Corp shall not be liable for any damages, losses, costs, or expenses, direct, indirect, or incidental, arising out of or related to the use of this material.

Technical Support

For further assistance, please contact Avenview Technical Support.