



# OmniStream™ Single-Channel / Dual-Channel Networked AV Encoder / Decoder

---

## Solutions Setup and Configuration Guide

AT-OMNI-232   AT-OMNI-311   AT-OMNI-111   AT-OMNI-121  
AT-OMNI-324   AT-OMNI-112   AT-OMNI-122

Atlona Manuals  
**Networked AV**

## Version Information

---

Version	Release Date	Notes
1	Feb 2019	Initial release
2	Mar 2019	Audio added
3	Mar 2019	USB added
4	May 2019	Added Network Switch Configuration, IR Control
5	Sept 2019	Updated <b>AMS</b> , <b>Updating Device Firmware</b> , and <b>Configuring OmniStream Devices</b> sections with firmware 2.5 screenshots
6	Aug 2020	Updated for AMS integration into Velocity with firmware version 2.1.0
7	Oct 2020	Updated for Velocity with Integrated AMS firmware version 2.2.0

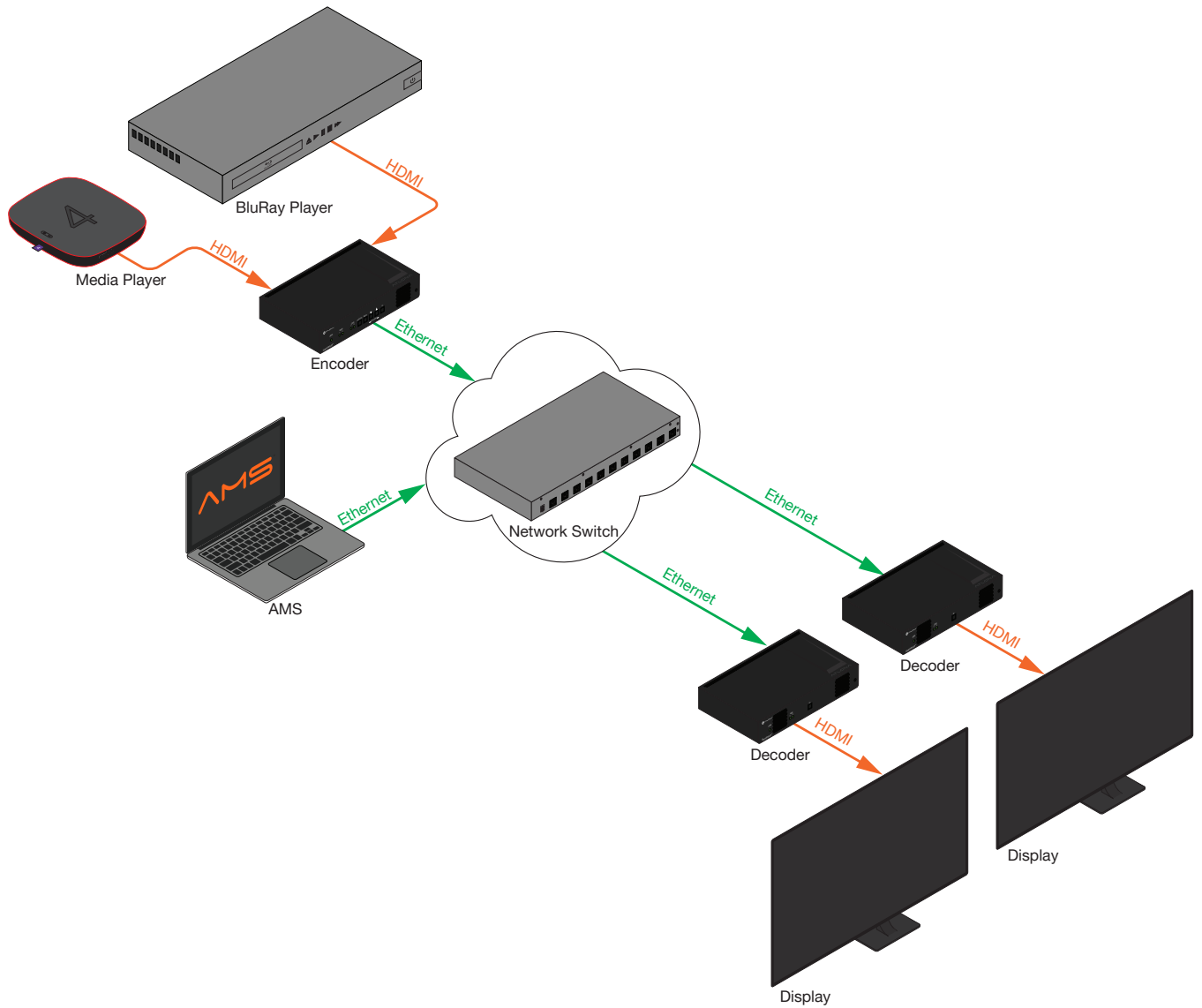
# Table of Contents

---

<b>Introduction</b>	<b>4</b>
<b>Getting Started</b>	<b>5</b>
Selecting a Network Switch	5
Velocity with Integrated AMS - Purchase or Download	5
Recommendations	5
<b>Connections</b>	<b>6</b>
<b>Network Switch Configuration</b>	<b>7</b>
Getting Started	7
VLAN Setup	9
IPv4 Interface and DHCP Setup	12
Port Mapping	18
Configuring IP Multicast	20
Creating User Accounts	24
<b>Velocity with Integrated AMS</b>	<b>26</b>
Getting an IP Address	26
Login	26
Updating	27
Discovery	29
<b>Updating Device Firmware</b>	<b>31</b>
<b>Configuring OmniStream Devices</b>	<b>32</b>
<b>Testing Connectivity</b>	<b>37</b>
<b>IR Control</b>	<b>38</b>
Controlling the Display using the Display's IR Remote	38
Required Equipment	39
Connecting the IR Receiver to the Encoder	39
Connecting the IR Emitter to the Decoder	40
Identifying the Encoder using Velocity with Integrated AMS	41
Configuring the Encoder Serial Port	42
Configuring the Encoder Session	43
Configuring the Decoder Serial Port	45
Testing IR Functionality	48
Controlling the Display using a Control System	49
<b>USB to IP Adapter</b>	<b>50</b>
<b>IP to Analog Audio Bridge</b>	<b>53</b>
<b>Video Walls</b>	<b>56</b>

# Introduction

This guide provides a base for setting up and configuring a small OmniStream™-based solution. The setup instructions will provide information for building a system capable of sending and receiving audio and video through OmniStream™ encoders and decoders, as well as a simple way to set up video walls and audio routing.



# Getting Started

## Selecting a Network Switch

A network switch will be needed to power and pass IP traffic. A list of certified switches is provided below with download links for prebuilt configurations. Atlona recommends using a switch from the certified list to ensure compatibility.

Certified Switcher	Download	Configuration
Cisco SG300-10MPP	<a href="#">Box Download Link</a>	The default configuration can be found within the OmniStream Certified Network Switches document that can be found at <a href="https://atlona.com/pdf/OmniStream_Certified_Switches.pdf">https://atlona.com/pdf/OmniStream_Certified_Switches.pdf</a> .
Cisco SG300-28MP	<a href="#">Box Download Link</a>	
Cisco SG300-52MP	<a href="#">Box Download Link</a>	
Cisco SG350-10MP	<a href="#">Box Download Link</a>	
Cisco SG350-28MP	<a href="#">Box Download Link</a>	
Cisco SG350-52MP	<a href="#">Box Download Link</a>	
Cisco SG550X-24MP	<a href="#">Box Download Link</a>	
Cisco SG550X-48MP	<a href="#">Box Download Link</a>	
Pakedge S3L-24P	<a href="#">Box Download Link</a>	
Luminex GigaCore 26i	<a href="#">Box Download Link</a>	
Ruckus ICX 7150-48ZP	<a href="#">Box Download Link</a>	
Ubiquiti ES-48-500W /ES-48-750W	<a href="#">Box Download Link</a>	

## Velocity with Integrated AMS - Purchase or Download

For configuration of the OmniStream devices with this guide, Velocity with integrated AMS (Atlona Management System) will be needed. AMS has two options: AT-VGW-HW-3/AT-VGW-HW-10/AT-VGW-HW-20 hardware (with integrated AMS) or AT-AMS-SW free software. AT-VGW-HW-3/10/20 can be purchased at: <https://atlona.com/product/vgw-hw/> or AT-AMS-SW free software can be downloaded from <https://atlona.com/product/at-ams-sw/>. AMS will be needed before progressing further into this setup and configuration guide.

## Recommendations

- When using multiple of the same OmniStream devices, or for reference, labeling can be used. It's best to place the label on the front of the device for visibility. When labeling, notate the last 4 numbers of the MAC address, found on the bottom of the unit on the label, for easier IP discovery and notation later.
- Use a component surge suppressor with line conditioning for best results.



**IMPORTANT:** Atlona's warranty does not cover damage due to electrical disturbances. A component surge suppressor with line conditioning is highly suggested, especially in areas with electrical storms.

## Connections

---

Initial connections can be done without installing the devices in their final locations. Have at least one source and display available to ensure video is passing between OmniStream devices. It is recommended these steps be followed in the order they are written.

1. Connect all devices to the network switch using a CAT5e or higher cable. OmniStream devices will need to be plugged into the PoE ports.
2. Have at least one source and display ready to connect to any of the OmniStream devices.
3. Once all the devices are connected to the network switch, connect the switch power supply to the power strip.
4. \*Optional\* If using the AT-OMNI-311, connect the USB B to USB A cable to the USB port of the PC, that will provide the 5V power.
5. \*Optional\* If using the AT-OMNI-324, connect the power supply from the unit to the power strip.
6. \*Optional\* If using the AT-VGW-HW, connect it to the network switch.
7. \*Optional\* Connect the power supply to the AT-VGW-HW and power strip.

# Network Switch Configuration

## Getting Started

Before working with the OmniStream devices, the network switch must be set up. This guide will provide instructions for configuring a **Cisco SG350X-24MP** switch. The following steps will be similar for most Cisco switches. However, there may be small variations, depending on the switch model. Consult the switch User Manual for more information.



**IMPORTANT:** The Network Switch Configuration chapter is divided into five sections. Each section must be followed in the order listed below. Deviating from this order, or skipping steps within a section, may result in unpredictable switch operation.

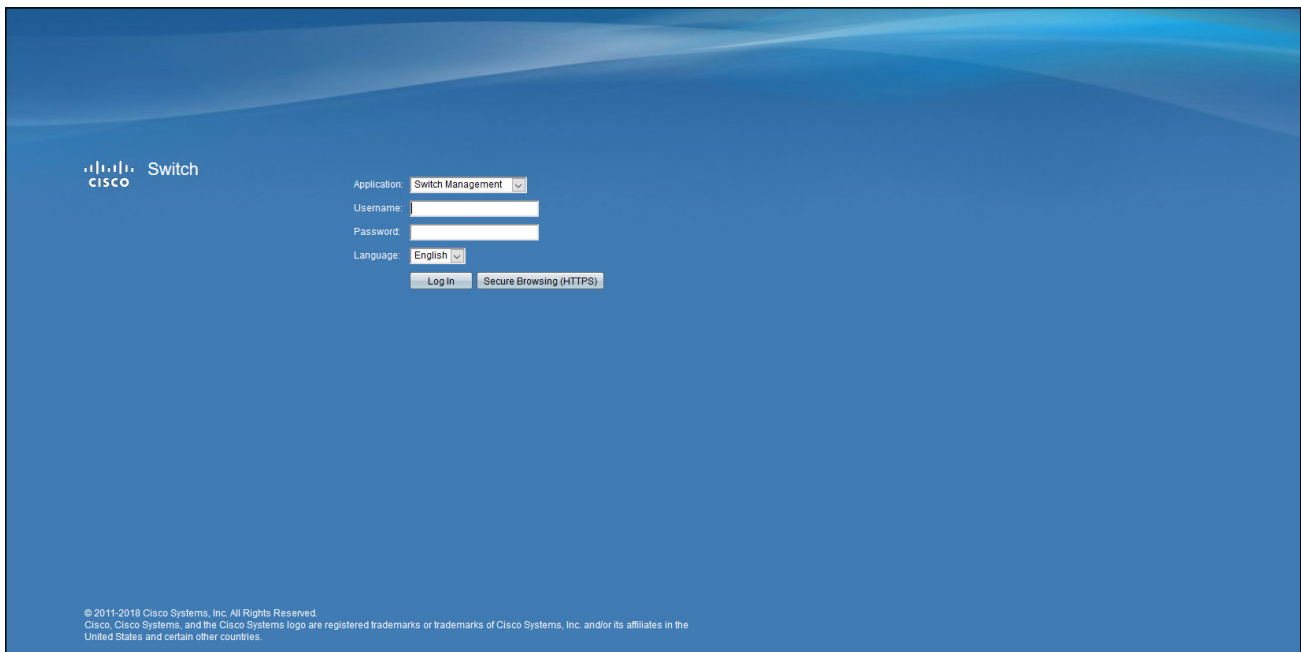
- VLAN Setup
- IPv4 Interface Setup
- Setting IP Multicast
- Setting up User Accounts

1. Connect a PC or laptop to the network switch. It is best to use the port that will remain on VLAN1 of the switch to avoid the PC losing connection when settings are changed on the switch.
2. Go into the computer settings and change the IP of the PC to be on the same range as the switch.



**NOTE:** If the IP address of the network switch is 192.168.1.254, then the computer should be set to 192.168.1.xx, where xx represents values from 1 to 253, as long as that IP address is not already assigned on that network. The default IP address for all Cisco switches is 192.168.1.254/24.

3. Launch the desired web browser and enter the IP address of the network switch into the address field, then press [ENTER].

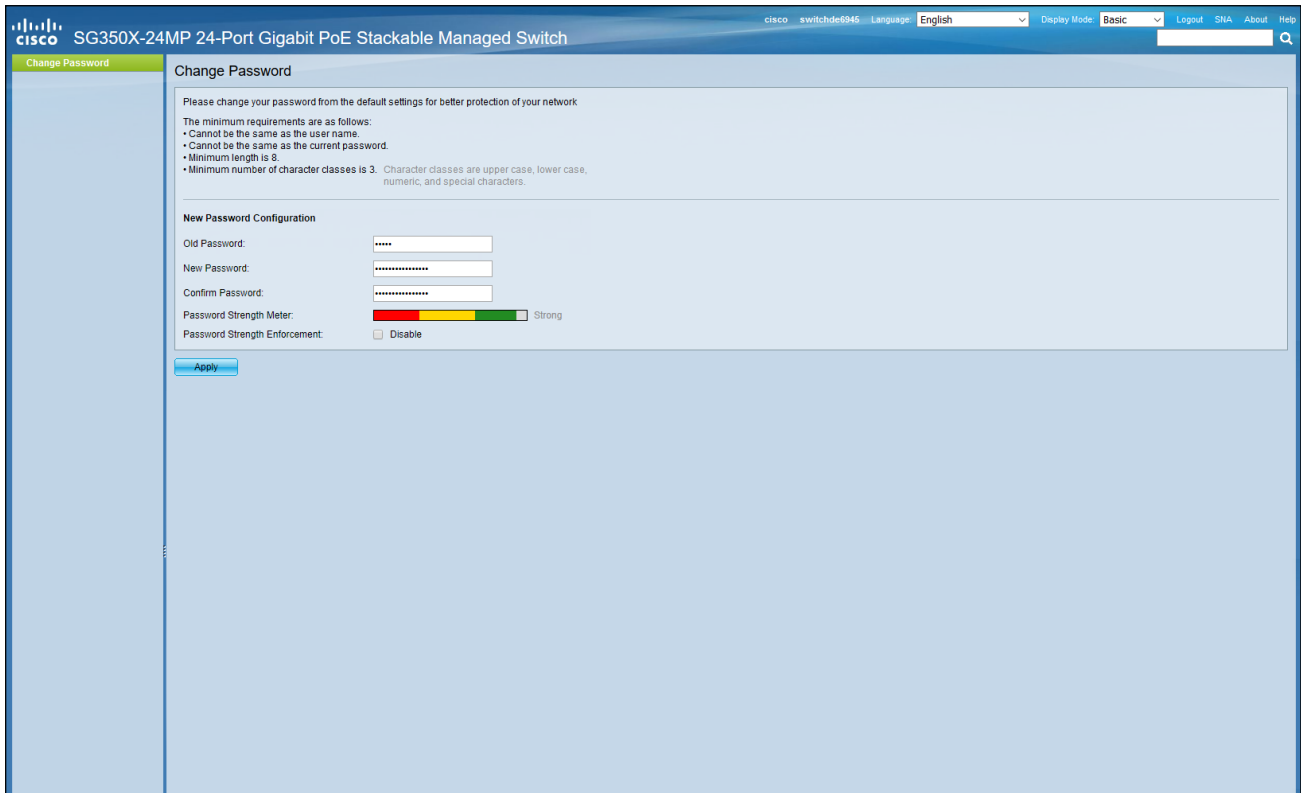


4. Enter the username and password. The default login credentials are as follows:

Username: cisco  
Password: cisco

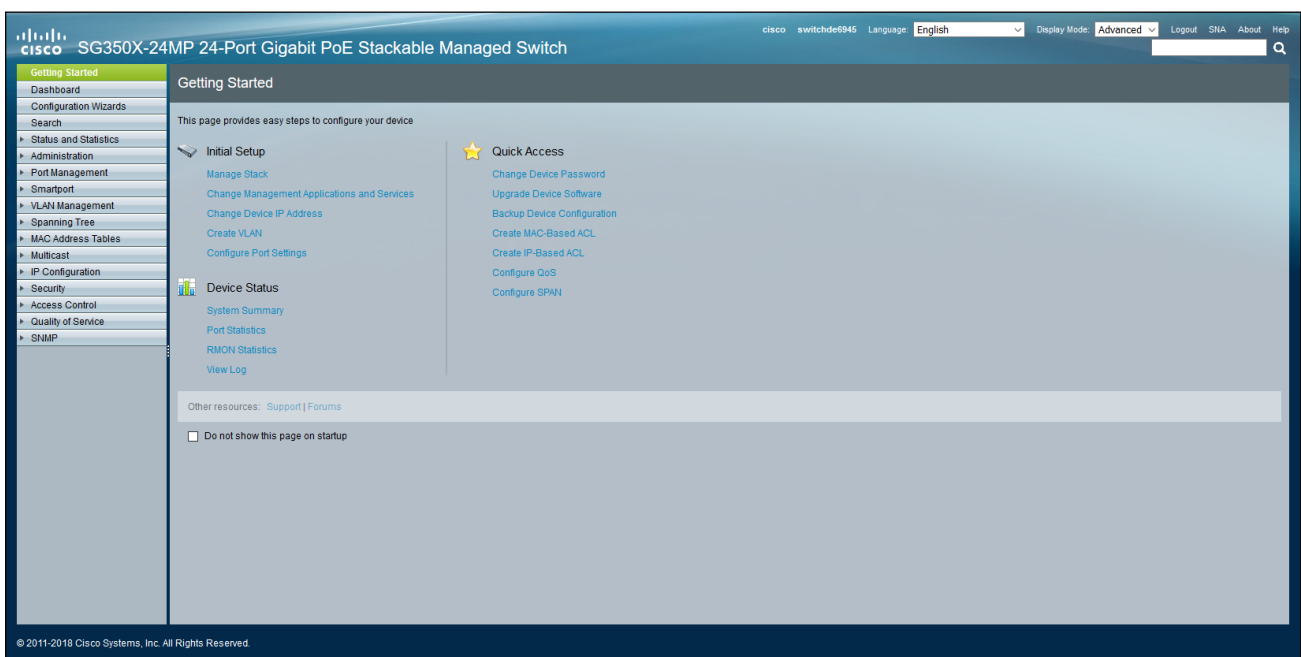
5. Click the **Login** button.

The switch will most likely require a new password to be assigned, before going further. This step may vary depending on the network switch. Enter the desired password, as required.



The screenshot shows the Cisco configuration interface for an SG350X-24MP switch. The 'Change Password' page is active, displaying instructions and a form for password configuration. The instructions state: 'Please change your password from the default settings for better protection of your network. The minimum requirements are as follows: • Cannot be the same as the user name. • Cannot be the same as the current password. • Minimum length is 8. • Minimum number of character classes is 3. Character classes are upper case, lower case, numeric, and special characters.' The form includes fields for 'Old Password', 'New Password', and 'Confirm Password', each with a masked input field. A 'Password Strength Meter' is shown with a green bar indicating 'Strong' strength. There is a 'Password Strength Enforcement' checkbox which is currently unchecked. An 'Apply' button is located at the bottom of the form.

6. Click the **Apply** button to commit changes.
7. The **Getting Started** page will be displayed.



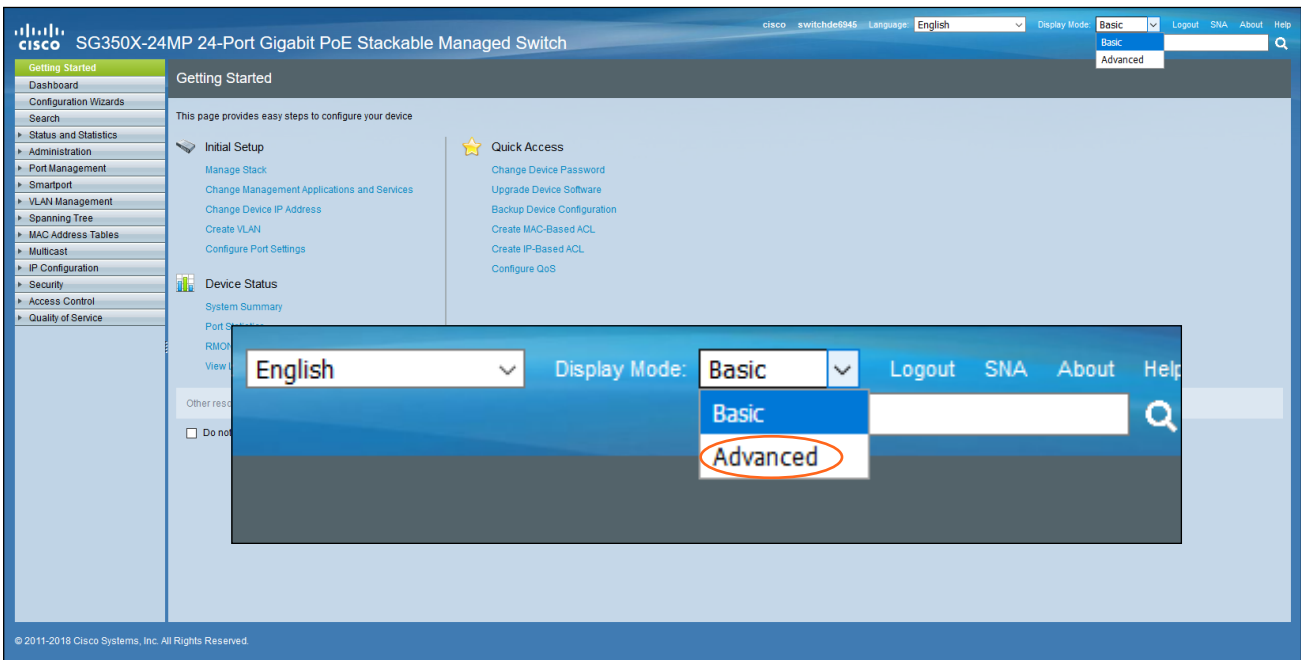
The screenshot shows the Cisco configuration interface for an SG350X-24MP switch, now displaying the 'Getting Started' page. The page title is 'Getting Started' and it includes the text: 'This page provides easy steps to configure your device'. The page is organized into three main sections: 'Initial Setup', 'Device Status', and 'Quick Access'. 'Initial Setup' includes links for 'Manage Stack', 'Change Management Applications and Services', 'Change Device IP Address', 'Create VLAN', and 'Configure Port Settings'. 'Device Status' includes links for 'System Summary', 'Port Statistics', 'RMON Statistics', and 'View Log'. 'Quick Access' includes links for 'Change Device Password', 'Upgrade Device Software', 'Backup Device Configuration', 'Create MAC-Based ACL', 'Create IP-Based ACL', 'Configure QoS', and 'Configure SPAN'. At the bottom, there are 'Other resources: Support | Forums' and a checkbox labeled 'Do not show this page on startup' which is currently unchecked. The footer of the page reads '© 2011-2018 Cisco Systems, Inc. All Rights Reserved'.



## VLAN Setup

The purpose of creating a VLAN is to separate a network into separate logical areas / broadcast domains. In this case, the VLAN is created to isolate AV-over-IP traffic from normal network traffic.

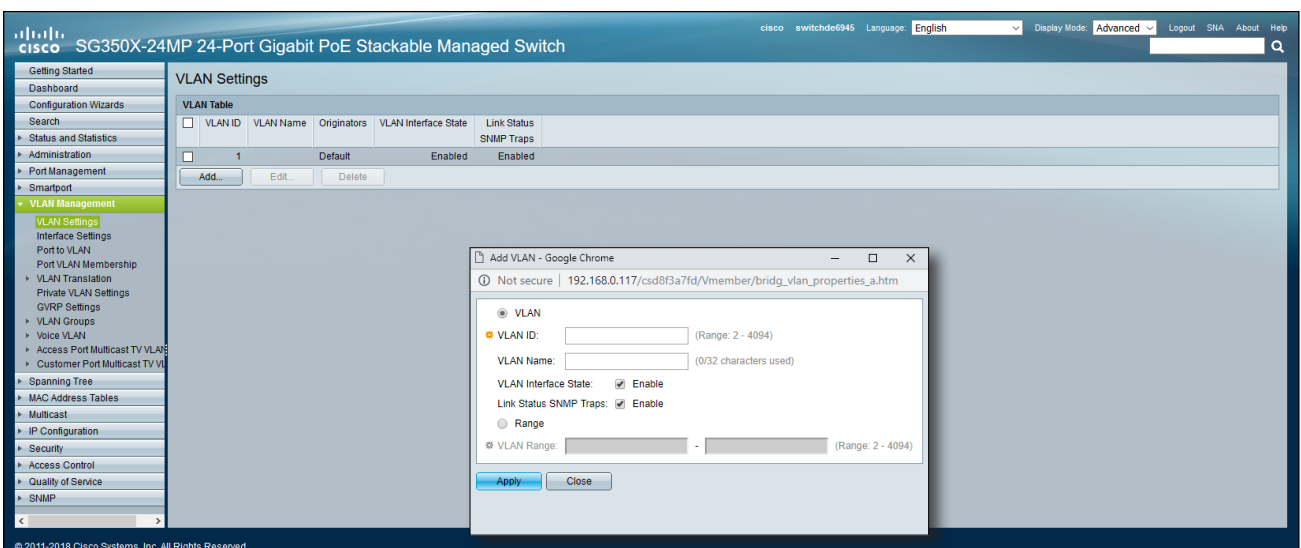
- Click the **Display Mode** drop-down list, near the upper-right hand corner of the screen, and select **Advanced**.



- Select **VLAN Management** from the menu on the left side of the screen. The **VLAN Management** menu will expand and the **VLAN Settings** page will be displayed. If the **VLAN Setting** page is not displayed, click **VLAN Management > VLAN Setting** to display the page.

By Default, VLAN 1 is active. If the network is self-contained, skip to 15. Otherwise, continue with the next step.

- Click the **Add...** button. The **Add VLAN** dialog will be displayed.



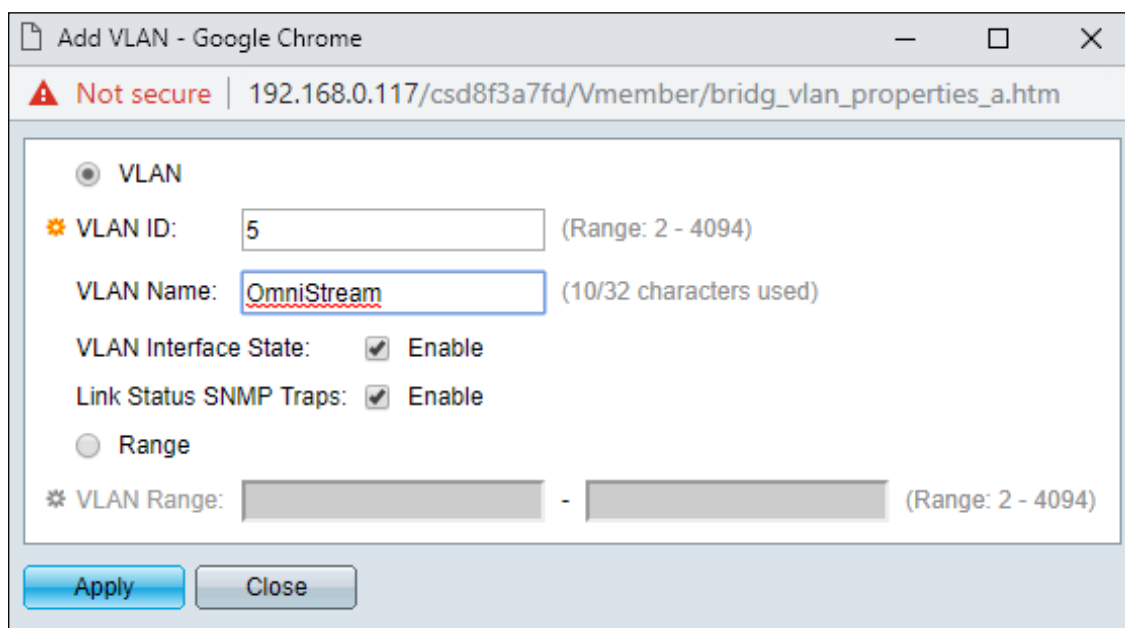
## Network Switch Configuration

11. Enter the numerical ID of the VLAN in the **VLAN ID** field. This value is required and must be within the range of 2 to 4094.

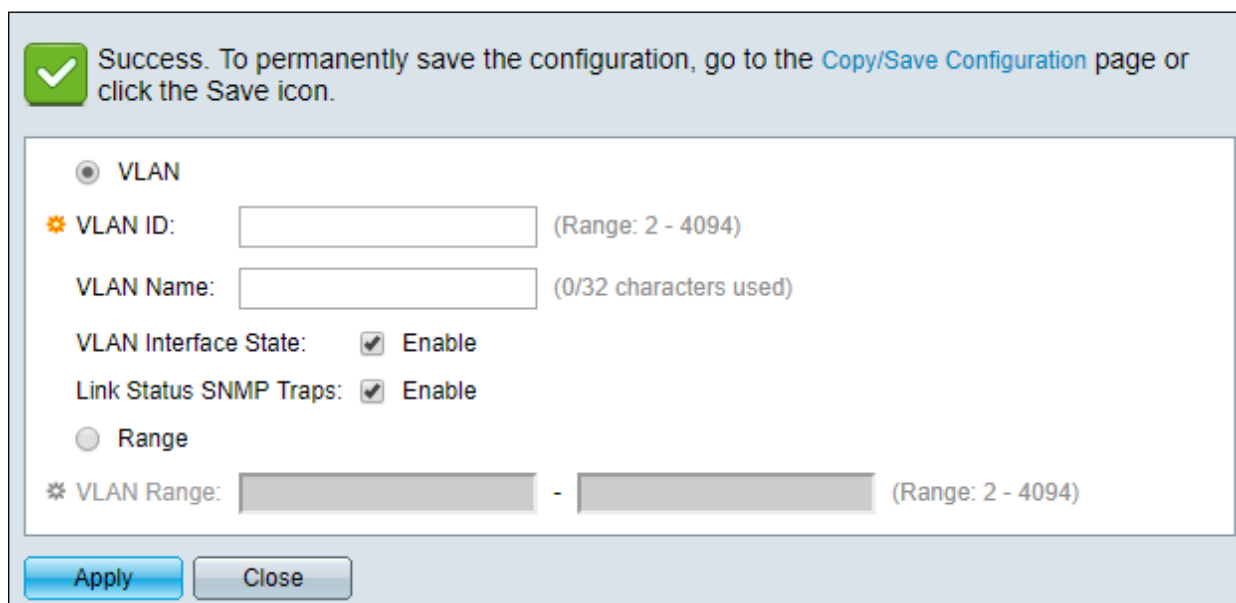


**NOTE:** VLAN 1 is the Cisco default VLAN. This VLAN can be used, but it cannot be modified or deleted.

12. OPTIONAL: Enter a name for the VLAN in the **VLAN Name** field. For example, the name of the VLAN could be used to identify a department, within a company, which uses that broadcast domain. In this example, “OmniStream” has been assigned as the name of VLAN 5.

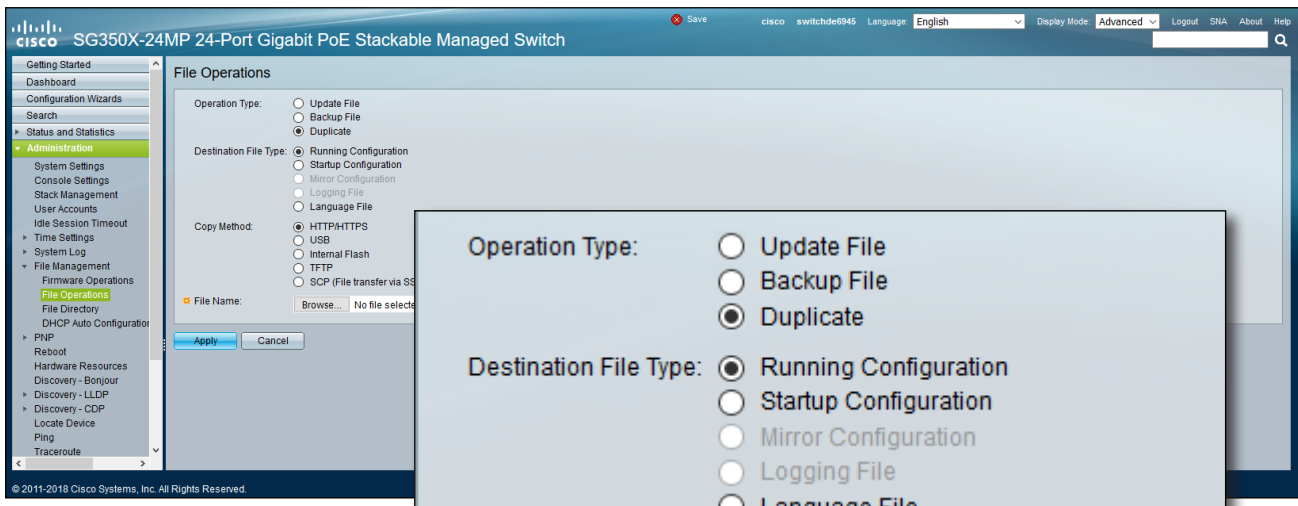


13. Click the **Apply** button to commit changes. If the VLAN was successfully created, the dialog box will display a “Success” message.

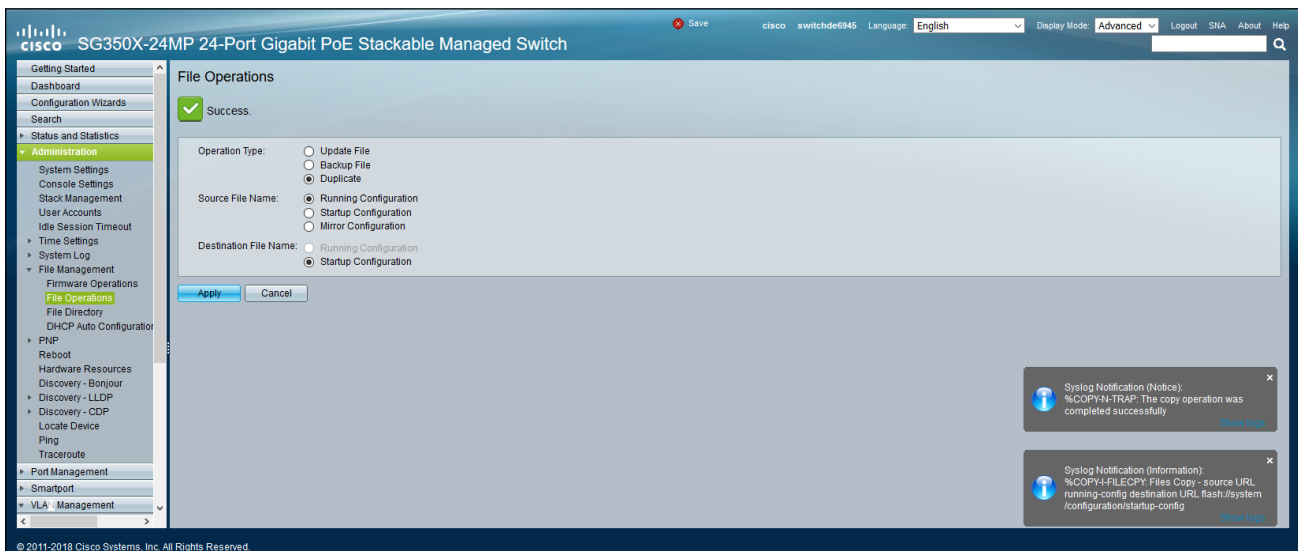


## Network Switch Configuration

14. Repeat steps 11 through 13 to create as many VLANs as needed. If no additional VLANs are required, click the **Close** button to dismiss the **Add VLAN** dialog box.
15. Click **Administration**, in the left-hand menu bar and select **File Operations**. The **File Operations** page will be displayed.
16. Click the **Duplicate** radio button, next to **Operation Type**.



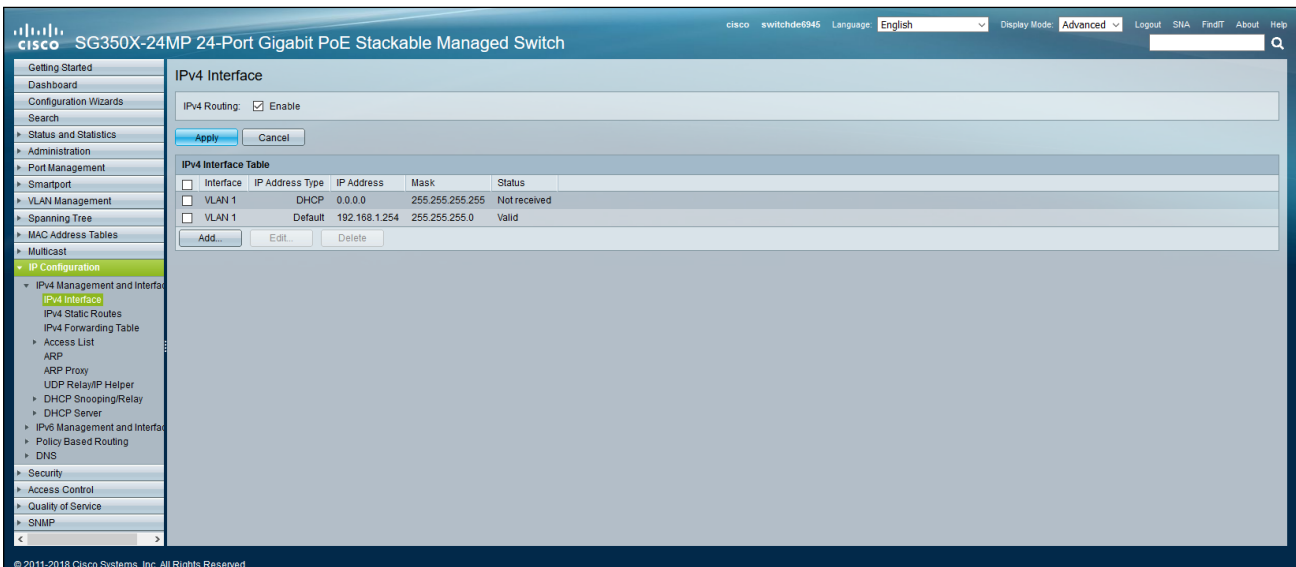
17. Click the **Apply** button to commit changes.



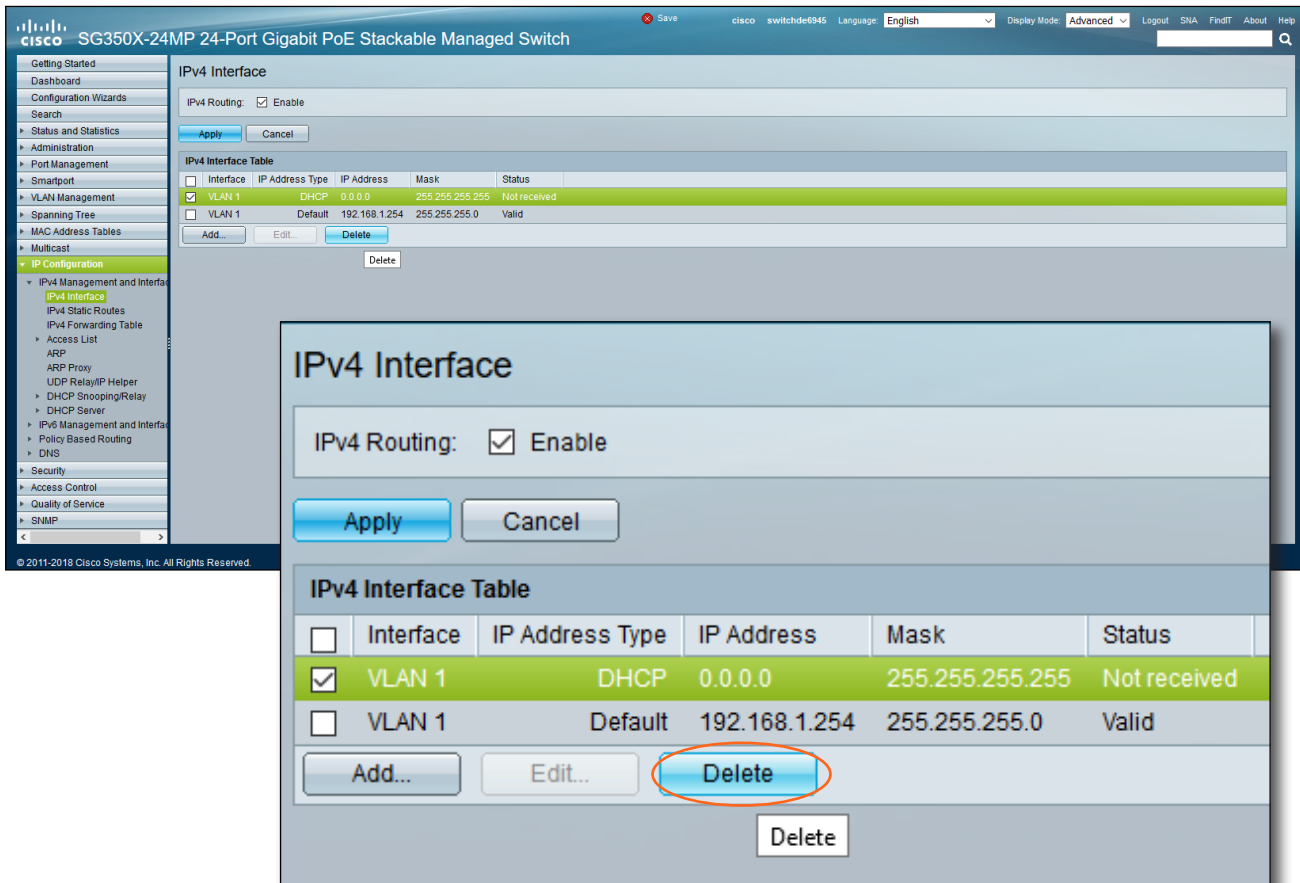
## IP Interface and DHCP Setup

The OmniStreams come with DHCP enabled. This section will configure the switch to become a DHCP server.

- Click **IP Configuration** in the left-hand menu bar and select **IPv4 Interface**. The **IPv4 Interface** page will be displayed.

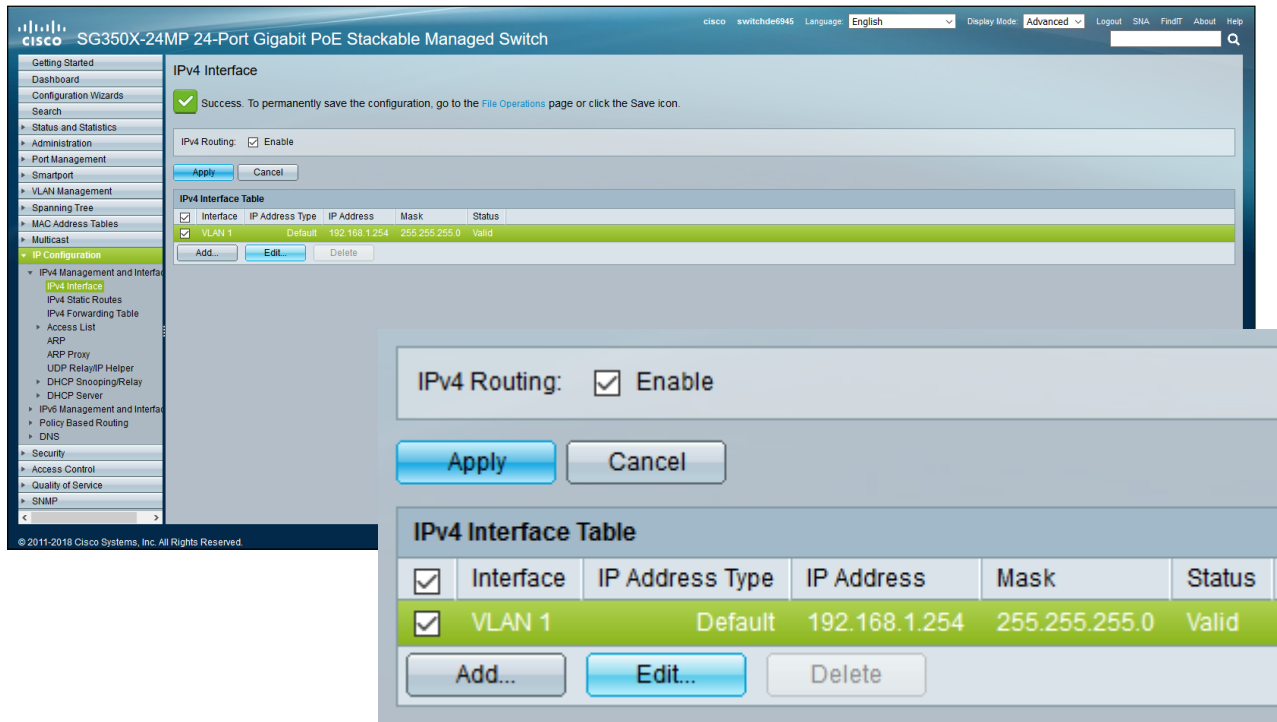


- Click the check box next to **VLAN 1** (DHCP) and then click the **Delete** button.



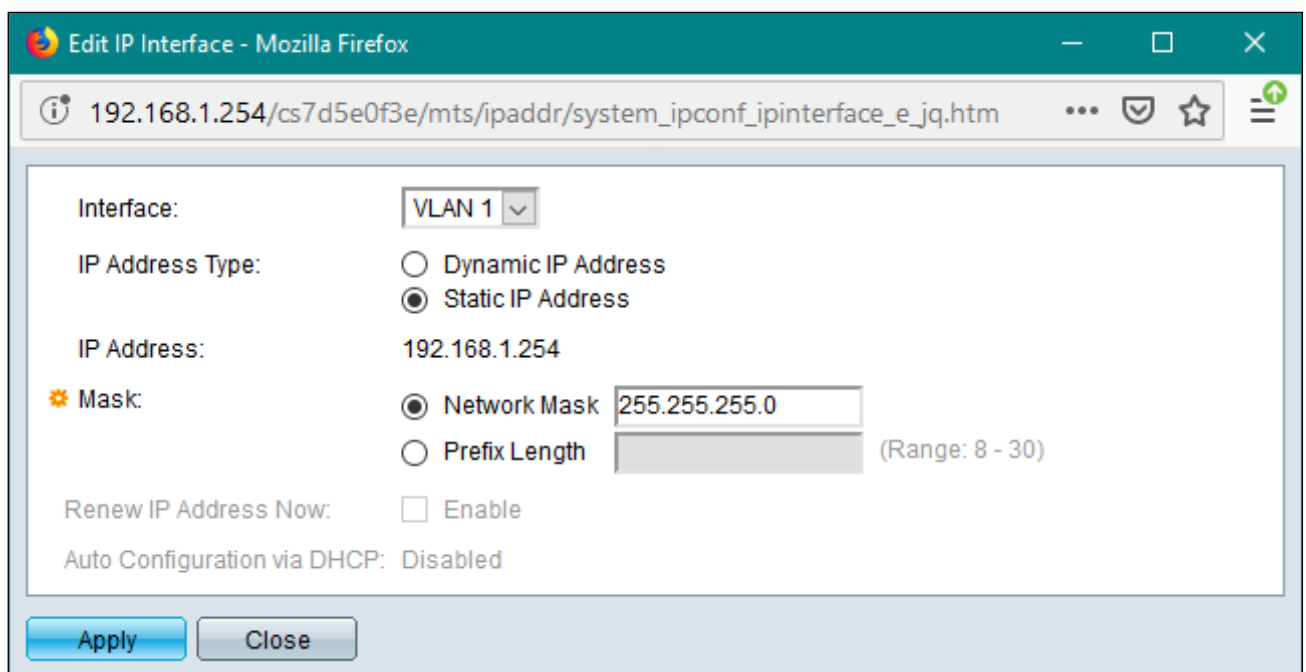
20. Check the IP settings for VLAN 1. If no changes are required, continue with Step 21. However, if a different IP address or subnet mask need to be specified, then follow the steps below:

- a. Click the check box next to **VLAN 1**.
- b. Click the **Edit** button.



The screenshot shows the Cisco configuration page for an SG350X-24MP switch. The 'IPv4 Interface' section is active, showing a success message and a table for the IPv4 Interface Table. The table has columns for Interface, IP Address Type, IP Address, Mask, and Status. The row for VLAN 1 is highlighted, showing a Static IP Address of 192.168.1.254 with a mask of 255.255.255.0. Below the table, there are 'Add...', 'Edit...', and 'Delete' buttons. A modal dialog box is overlaid on the page, showing the 'Edit IP Interface' configuration for VLAN 1. The dialog has a title bar 'Edit IP Interface - Mozilla Firefox' and a URL bar. The configuration fields are: Interface (VLAN 1), IP Address Type (Static IP Address selected), IP Address (192.168.1.254), Mask (Network Mask selected with 255.255.255.0 entered), Renew IP Address Now (unchecked), and Auto Configuration via DHCP (Disabled). 'Apply' and 'Close' buttons are at the bottom.

- c. The **Edit IP Interface** dialog will be displayed.
- d. Make make the required changes, then click the **Apply** button to commit changes.
- e. Click the **Close** button to dismiss the **Edit IP Interface** dialog box.



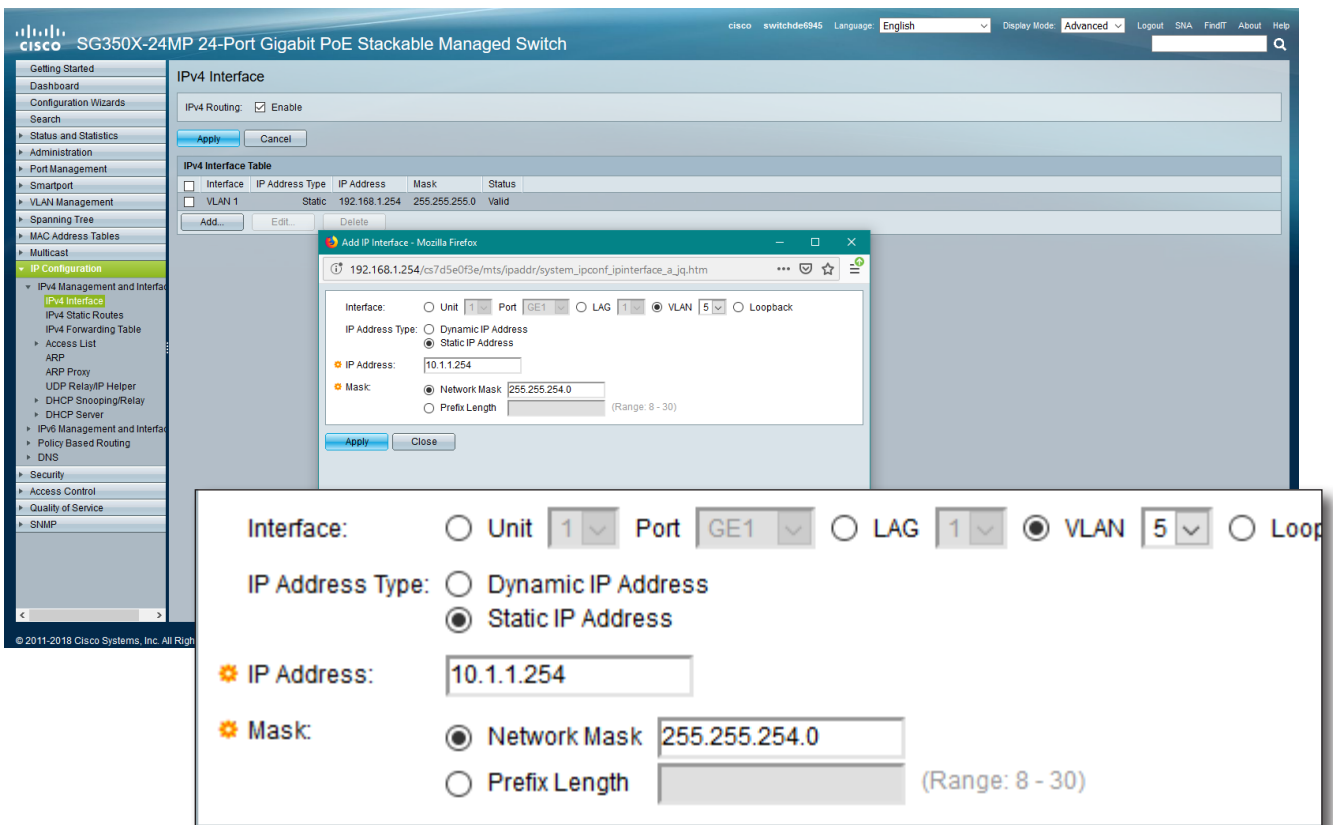
The screenshot shows the 'Edit IP Interface' dialog box in a Mozilla Firefox browser window. The dialog has a title bar 'Edit IP Interface - Mozilla Firefox' and a URL bar. The configuration fields are: Interface (VLAN 1), IP Address Type (Static IP Address selected), IP Address (192.168.1.254), Mask (Network Mask selected with 255.255.255.0 entered), Renew IP Address Now (unchecked), and Auto Configuration via DHCP (Disabled). 'Apply' and 'Close' buttons are at the bottom.

21. Click the **Add...** button. The **Add IP Interface** dialog box will be displayed.
22. Click the VLAN radio button, then click the drop-down list to select the VLAN that was created under **VLAN Setup** (page 9).
23. Click the **Static IP Address** radio button.



**NOTE:** It is recommended that a static IP address be assigned to a VLAN, to avoid IP changes.

24. Enter the IP address of the VLAN, in the **IP Address** field. In the example below, 10.1.1.254 is used. However, any available IP address in the pool may be used.
25. Click the **Network Mask** radio button and enter the subnet mask. In this example, 255.255.254.0 is used. However, depending upon the requirements, any valid network mask may be used.

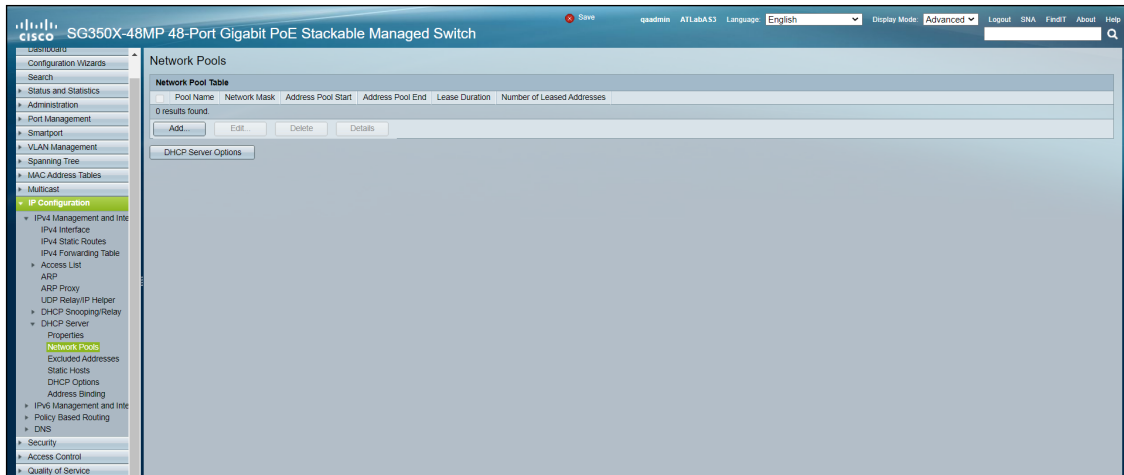


The screenshot shows the Cisco configuration interface for a switch. The 'Add IP Interface' dialog box is open, displaying the following configuration details:

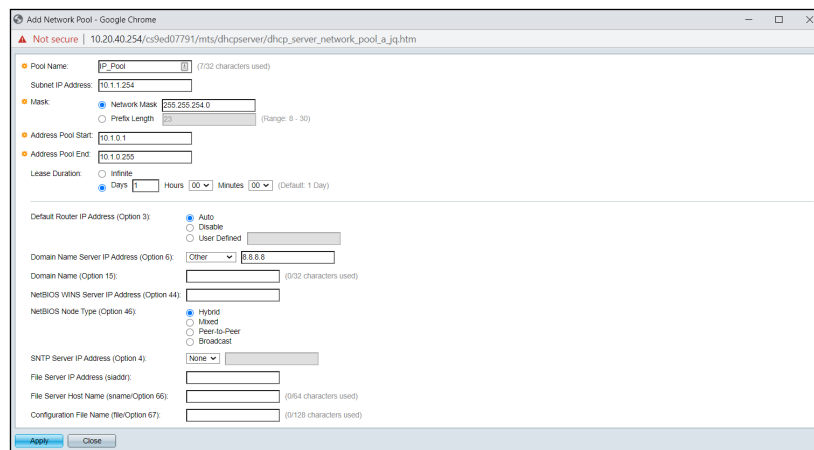
- Interface:**  Unit 1  Port GE1  LAG 1  VLAN 5  Loopback
- IP Address Type:**  Dynamic IP Address  Static IP Address
- IP Address:** 10.1.1.254
- Mask:**  Network Mask 255.255.254.0  Prefix Length (Range: 8 - 30)

26. Click the **Apply** button to commit changes. Repeat Steps 21 through 25 for each additional VLAN, as necessary.
27. After all VLANs have been set up, click the **Close** button to dismiss the **Add IP Interface** dialog box.

28. Click **DHCP Server** in the left-hand menu bar under IP Configuration and select **Network Pools**. The **Network Pools** page will be displayed.



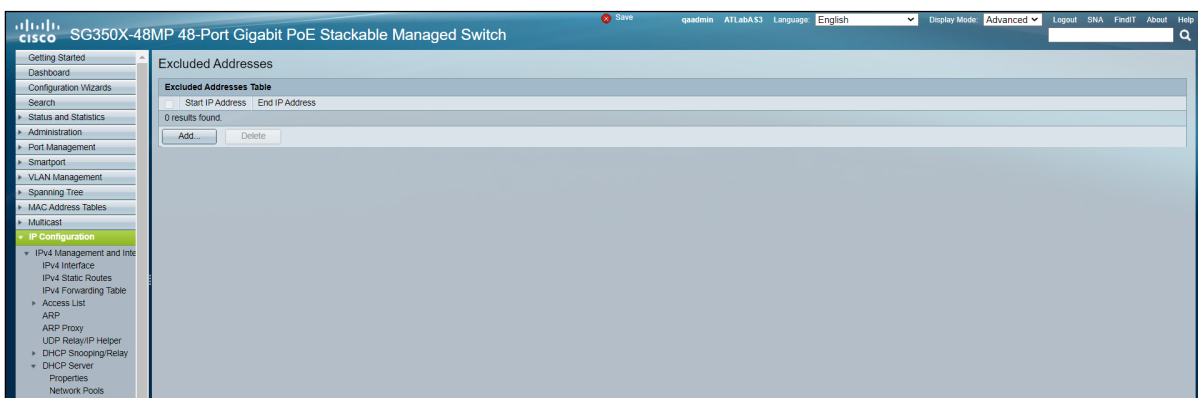
29. Click the **Add...** button. A new pop up will appear.



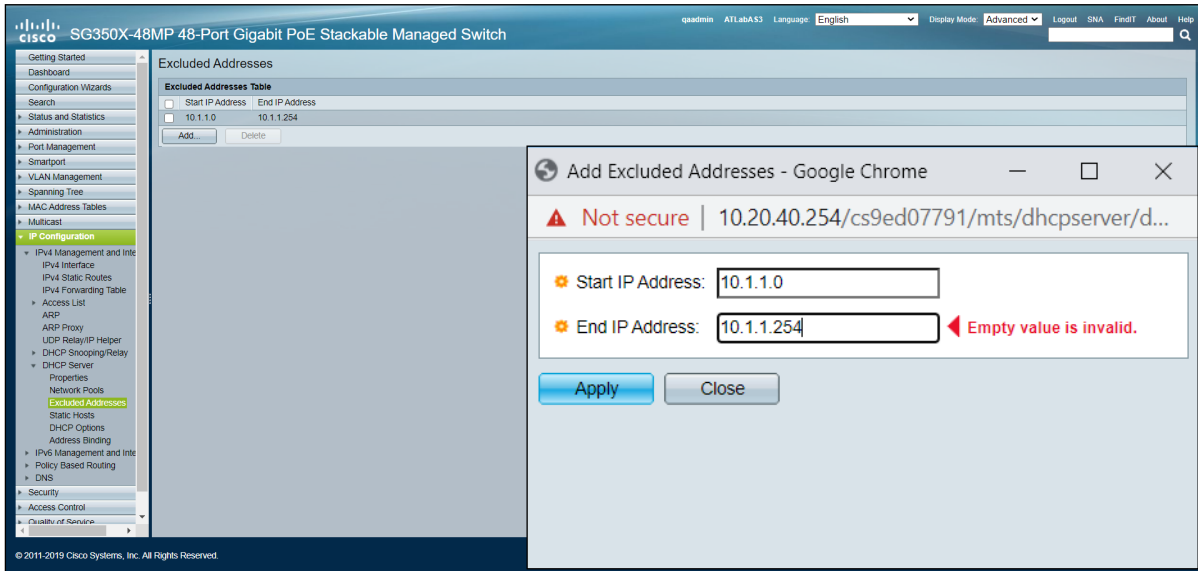
30. Enter the Pool Name, Subnet IP Address, and Network Mask.
31. Enter starting and ending IP addresses in to the **Address Pool Start** and **Address Pool End** fields.
32. Select the **Apply** button. The pop up window will close.

**NOTE:** Steps 33 through 36 are optional and should only be used if there is a set of IP addresses that need to be excluded from the server. If unneeded, skip to Step 37.

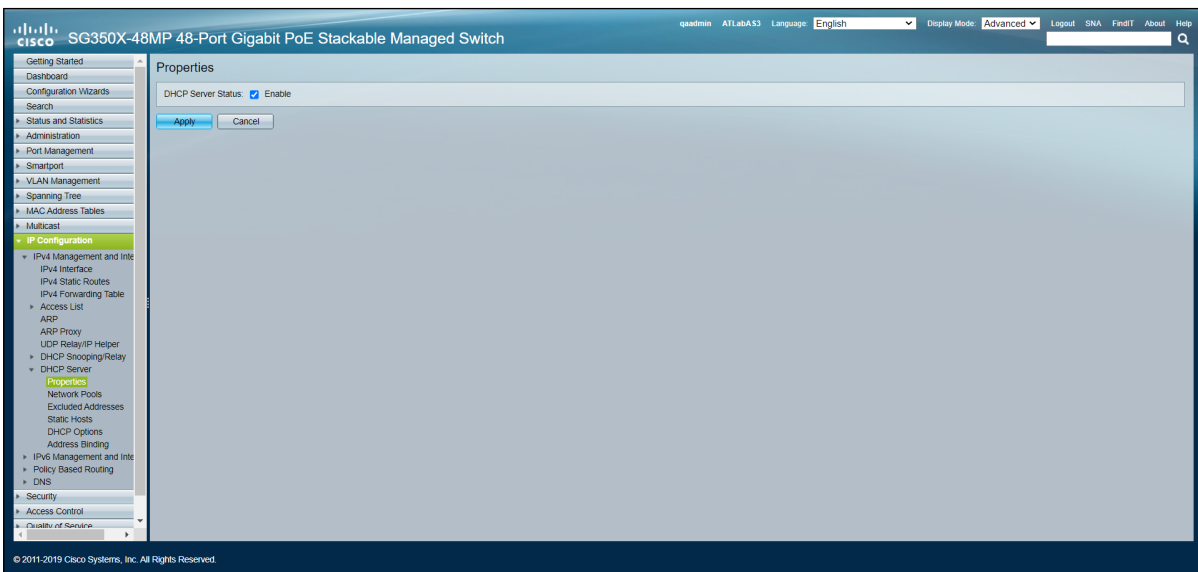
33. Select **Excluded Addresses** from under DHCP servers in the left side menu. The new page will open.



34. Enter any IP address range that the DHCP server will NOT assign to devices.
35. Press the **Apply** button.
36. Repeat for any/all IP ranges that should be excluded.



37. Click **Properties** in the left-hand menu bar from the DHCP Server menu. The new page will open.

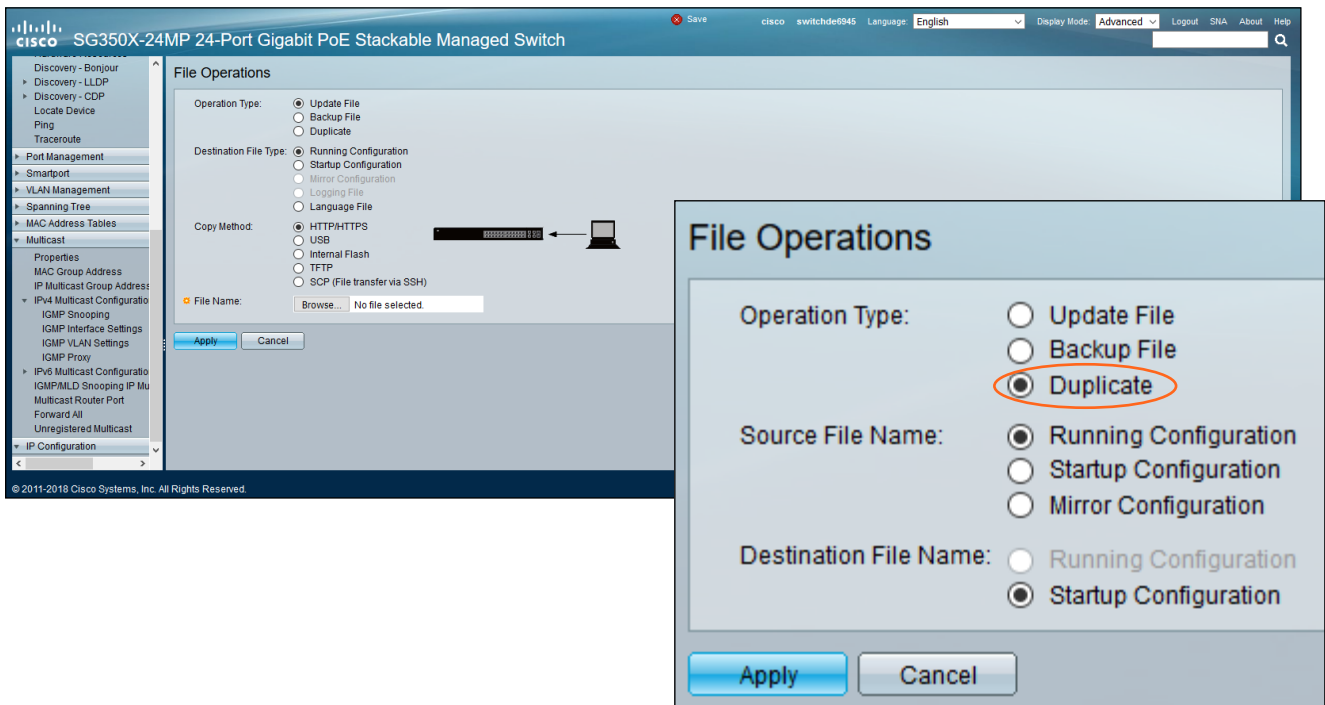


38. Check the box next to **Enable** and press **Apply** to turn the unit into a DHCP server.



## Network Switch Configuration

39. Click **Administration**, in the left-hand menu bar and select **File Operations**. The **File Operations** page will be displayed.
40. Click the **Duplicate** radio button, next to **Operation Type**.

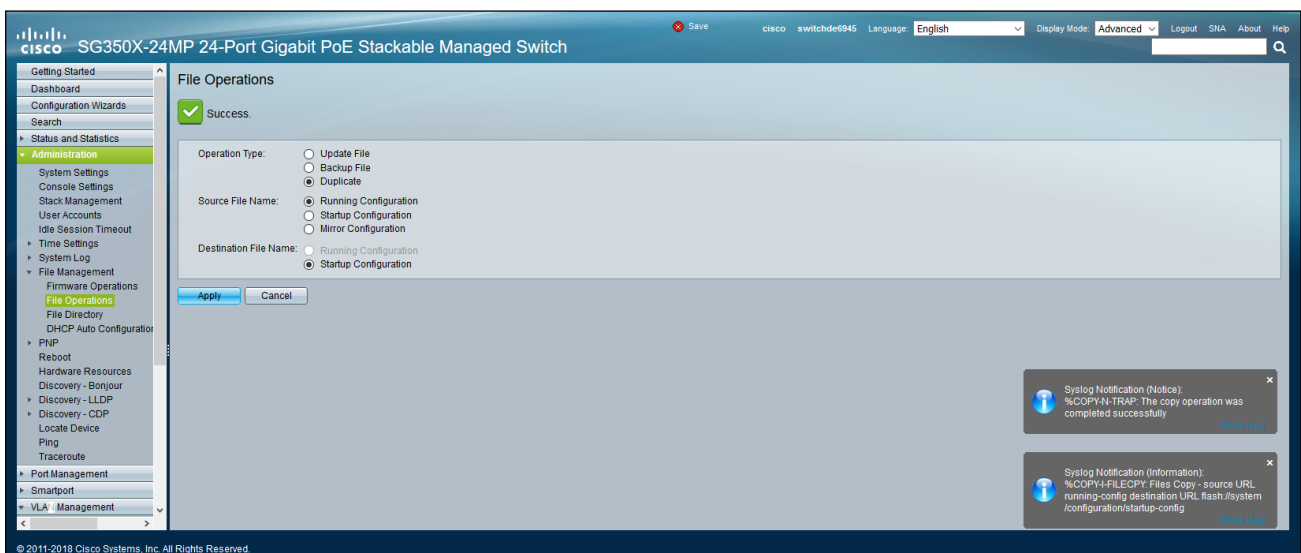


The screenshot shows the Cisco SG350X-24MP 24-Port Gigabit PoE Stackable Managed Switch interface. The left-hand menu bar has 'Administration' selected, and 'File Operations' is visible in the main content area. The 'File Operations' page displays the following configuration:

- Operation Type:**
  - Update File
  - Backup File
  - Duplicate
- Destination File Type:**
  - Running Configuration
  - Startup Configuration
  - Mirror Configuration
  - Logging File
  - Language File
- Copy Method:**
  - HTTP/HTTPS
  - USB
  - Internal Flash
  - TFTP
  - SCP (File Transfer via SSH)
- File Name:** Browse... No file selected.

An 'Apply' button is visible at the bottom left of the page. A modal dialog box titled 'File Operations' is overlaid on the page, showing the same configuration as the main page, but with 'Duplicate' selected under 'Operation Type', 'Running Configuration' selected under 'Source File Name', and 'Startup Configuration' selected under 'Destination File Name'. The 'Apply' and 'Cancel' buttons are also present in the modal dialog.

41. Click the **Apply** button to commit changes.



The screenshot shows the Cisco SG350X-24MP 24-Port Gigabit PoE Stackable Managed Switch interface after the 'Apply' button has been clicked. The left-hand menu bar has 'Administration' selected, and 'File Operations' is visible in the main content area. The 'File Operations' page displays the following configuration:

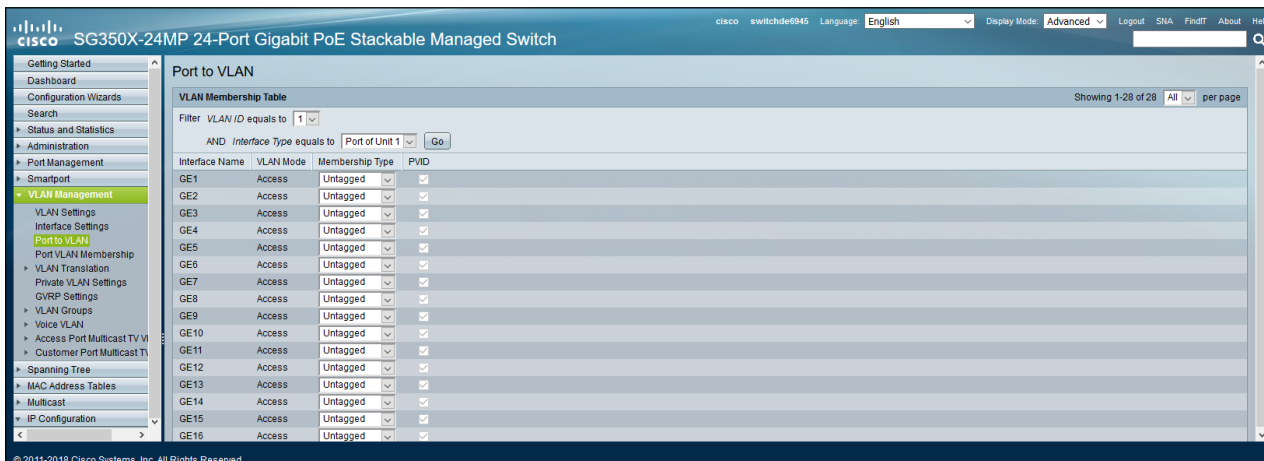
- Operation Type:**
  - Update File
  - Backup File
  - Duplicate
- Source File Name:**
  - Running Configuration
  - Startup Configuration
  - Mirror Configuration
- Destination File Name:**
  - Running Configuration
  - Startup Configuration

The 'Apply' button is now disabled. A 'Success' message is displayed at the top of the page. Two system notification messages are visible in the bottom right corner:

- System Notification (Notice):** %COPY-N-TRAP: The copy operation was completed successfully.
- System Notification (Information):** %COPY-F-FILECOPY: Files Copy - source URL running-config destination URL flash:/system /configuration/startup-config.

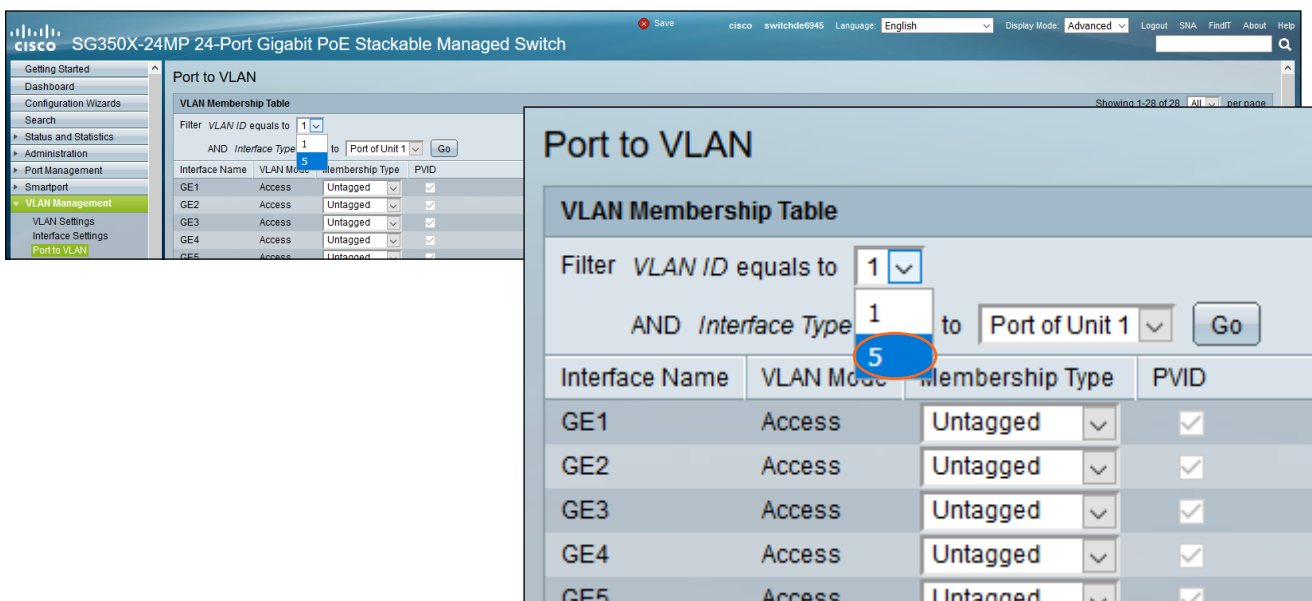
## Port Mapping

42. Click **Port to VLAN** from the **VLAN Management** menu. By default, the **Membership Type**, for each physical port (interface), is assigned as **Untagged**.

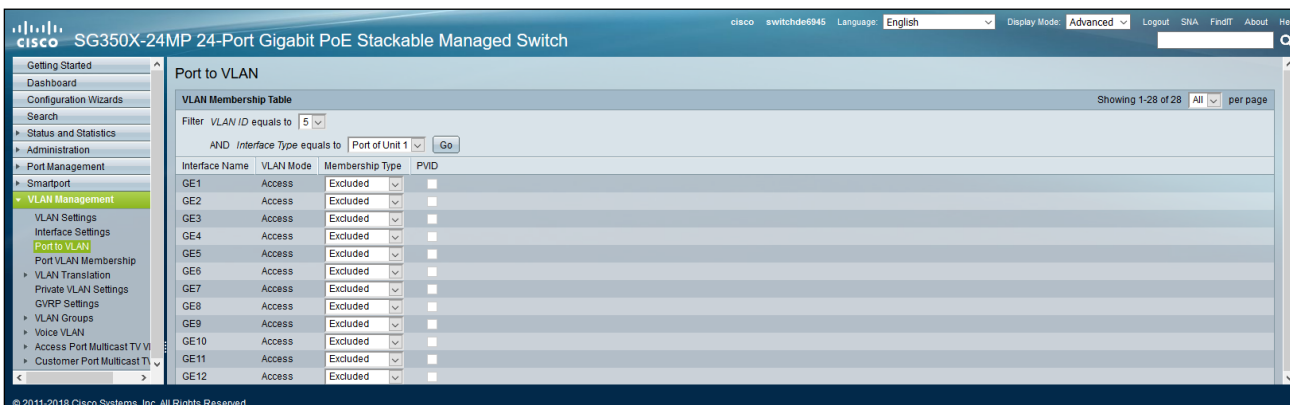


43. Click **VLAN ID equals to** drop-down list and select the VLAN ID that was created under **VLAN Setup** (page 9).

44. Leave the **AND Interface Type equals to** drop-down list as **Port of Unit 1**. Click the **Go** button.



45. The **Membership Type**, for the VLAN, will automatically be assigned as **Excluded** for each physical port on the switch.



46. Determine which physical ports will use the selected VLAN. Click the **Membership Type** drop-down list for each physical port that will use the VLAN, and set its value to **Untagged**. For example, if physical ports 6 and 7 will be used for VLAN 5, then set the **Membership Type** for these two ports to **Untagged**.

### Port to VLAN

**VLAN Membership Table**

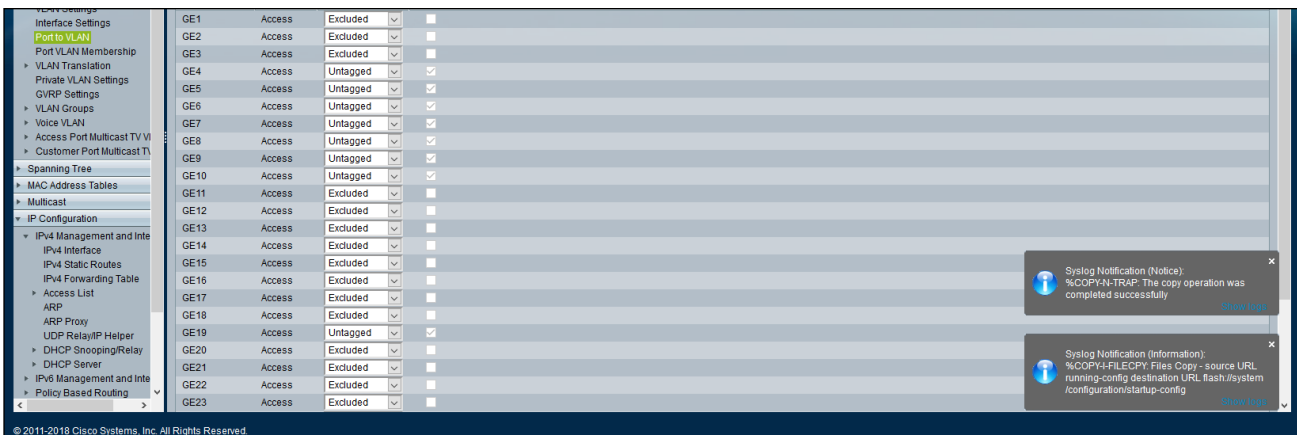
Filter VLAN ID equals to  Go

AND Interface Type equals to  Go

Interface Name	VLAN Mode	Membership Type	PVID
GE1	Access	Excluded <span style="float: right;">▼</span>	<input type="checkbox"/>
GE2	Access	Excluded	<input type="checkbox"/>
GE3	Access	Untagged	<input type="checkbox"/>
GE4	Access	Multicast TV VLAN	<input type="checkbox"/>
GE5	Access	Excluded <span style="float: right;">▼</span>	<input type="checkbox"/>

47. Scroll to the bottom of the list of ports and click the **Apply** button. Success messages will appear at the top and bottom right of the screen.

**NOTE:** If the port the PC is connected to is moved off VLAN1 to another VLAN (say VLAN5), then the PC will need to be set to the IP settings of the new VLAN to continue.

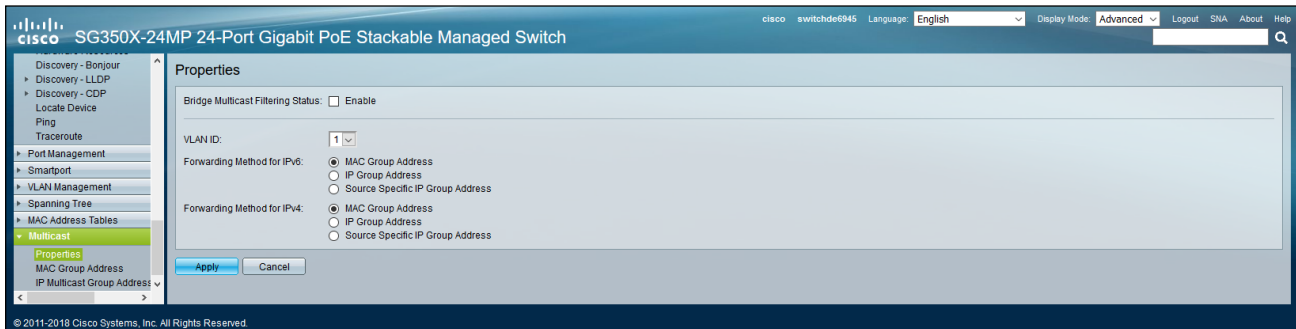


The screenshot shows the 'Port to VLAN' configuration page. The table lists ports GE1 through GE23. The 'Membership Type' for GE3 is set to 'Untagged'. Two Syslog Notification messages are visible in the bottom right corner:

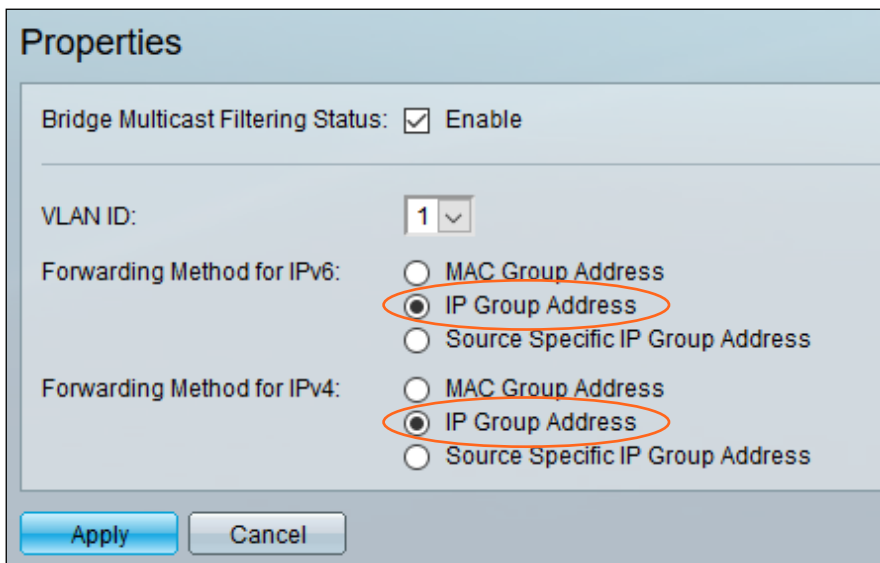
- Syslog Notification (Notice): %COPY:RTRAP: The copy operation was completed successfully
- Syslog Notification (Information): %COPY:FILECOPY: Files Copy - source URL /running-config destination URL flash:/system/running-config/startup-config

## Configuring IP Multicast

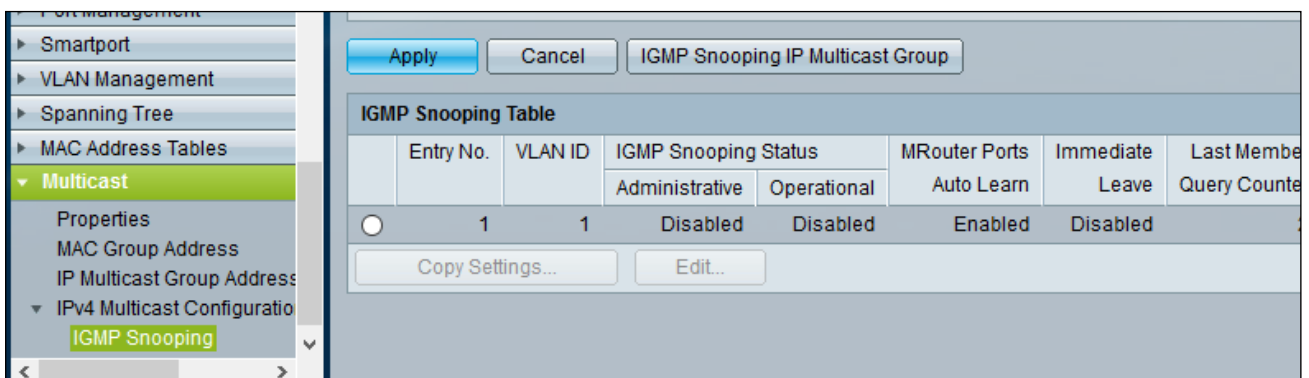
48. Click **Multicast** from the menu bar on the left side of the screen. The **Properties** window will automatically be displayed.



49. Click the **Enable** box, next to **Bridge Multicast Filtering Status**, to enable this feature.
50. Click the **IP Group Address** radio button, under both **Forwarding Method for IPv6** and **Forwarding Method for IPv4**.



51. Click the **Apply** button to commit changes.
52. Repeat steps 38 and 39 for each VLAN.
53. Click **IGMP Snooping**, under **IPv4 Multicast Configuration**, from the menu bar on the left side of the screen.



54. Click the check box next to **IGMP Snooping**, to enable this feature.
55. Click the **Apply** button to commit changes.

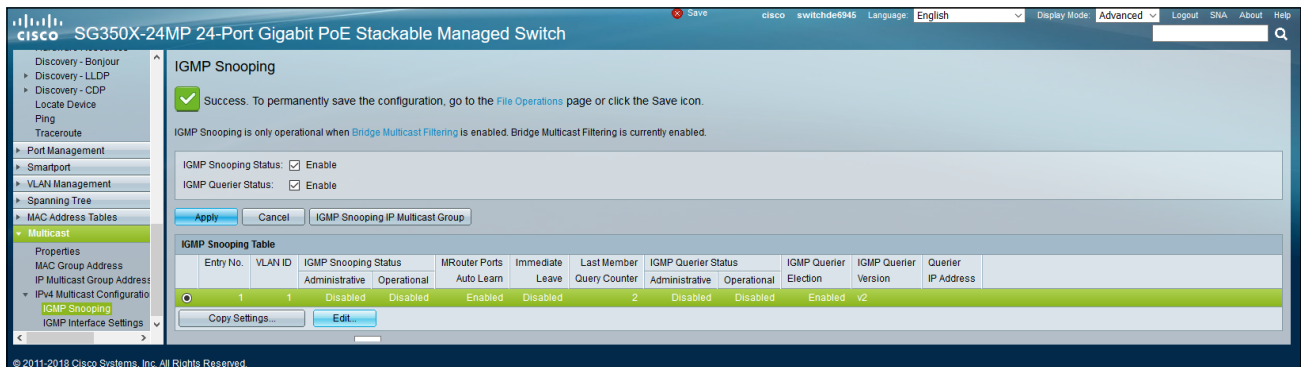
### IGMP Snooping

IGMP Snooping is only operational when [Bridge Multicast Filtering](#) is enabled. Bridge Multicast Filtering is currently enabled.

IGMP Snooping Status:  Enable

IGMP Querier Status:  Enable

56. Click the radio button next to **VLAN 1**, as shown below, in the **IGMP Snooping Table**.



Success. To permanently save the configuration, go to the [File Operations](#) page or click the Save icon.

IGMP Snooping is only operational when [Bridge Multicast Filtering](#) is enabled. Bridge Multicast Filtering is currently enabled.

IGMP Snooping Status:  Enable

IGMP Querier Status:  Enable

Entry No.	VLAN ID	Administrative	Operational	MRouter Ports Auto Learn	Immediate Leave	Last Member Query Counter	IGMP Querier Status Administrative	IGMP Querier Status Operational	IGMP Querier Election	IGMP Querier Version	Querier IP Address
<input checked="" type="radio"/>	1	1	Disabled	Disabled	Enabled	Disabled	2	Disabled	Disabled	Enabled	v2

57. Click the **Edit...** button to display the **Edit IGMP Snooping Settings** dialog box.

### Edit IGMP Snooping Settings - Mozilla Firefox

192.168.1.254/csafa621c4/multicast/igmp\_snooping\_e\_jq.htm

VLAN ID:

IGMP Snooping Status:  Enable

MRouter Ports Auto Learn:  Enable

Immediate Leave:  Enable

Last Member Query Counter:  Use Query Robustness (2)  
 User Defined  (Range: 1 - 7)

---

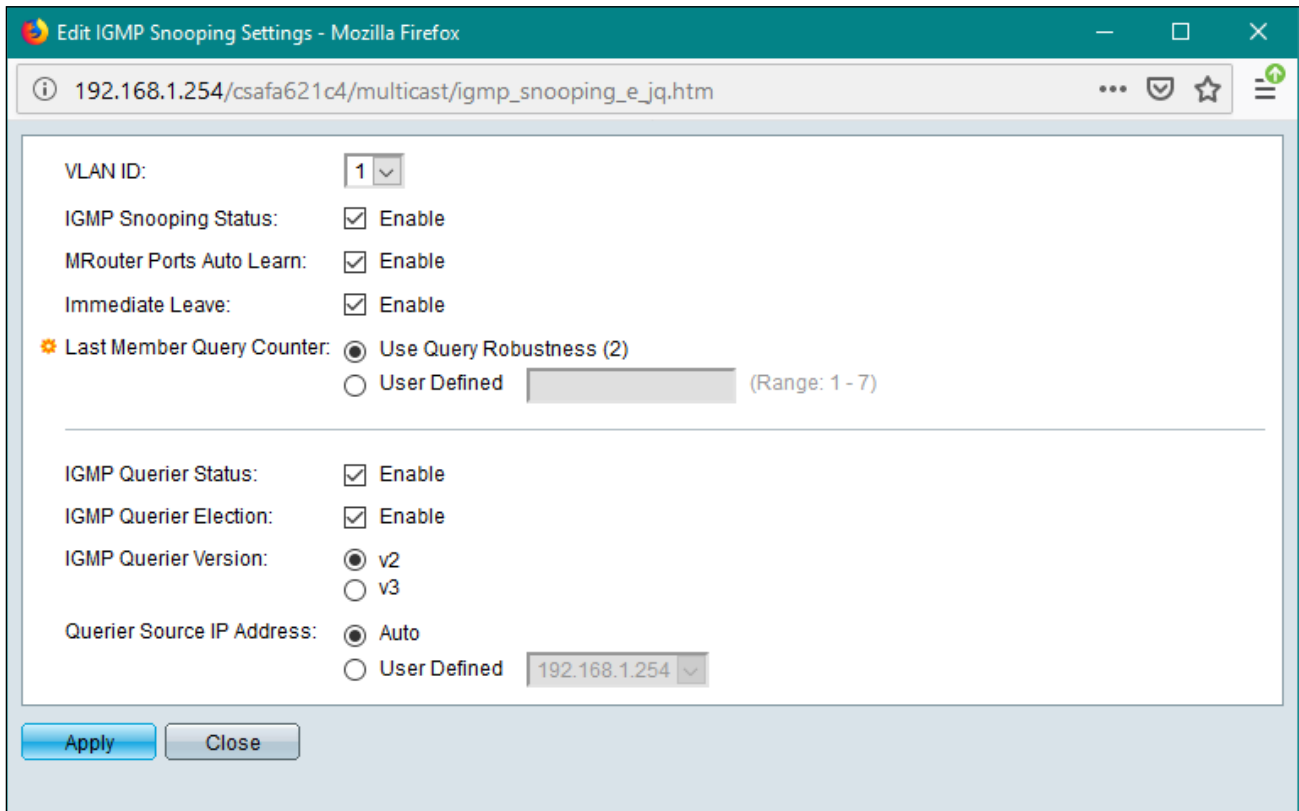
IGMP Querier Status:  Enable

IGMP Querier Election:  Enable

IGMP Querier Version:  v2  
 v3

Querier Source IP Address:  Auto  
 User Defined

58. Click the **Enable** checkboxes next to **IGMP Snooping Status**, **Immediate Leave**, and **IGMP Querier Status**. Make sure each of these checkboxes display a checkmark. Leave the rest of the settings as they are.
59. Click the **Apply** button to commit changes.



Edit IGMP Snooping Settings - Mozilla Firefox  
 192.168.1.254/csafa621c4/multicast/igmp\_snooping\_e\_jq.htm

VLAN ID:

IGMP Snooping Status:  Enable

MRouter Ports Auto Learn:  Enable

Immediate Leave:  Enable

Last Member Query Counter:  Use Query Robustness (2)  
 User Defined  (Range: 1 - 7)

---

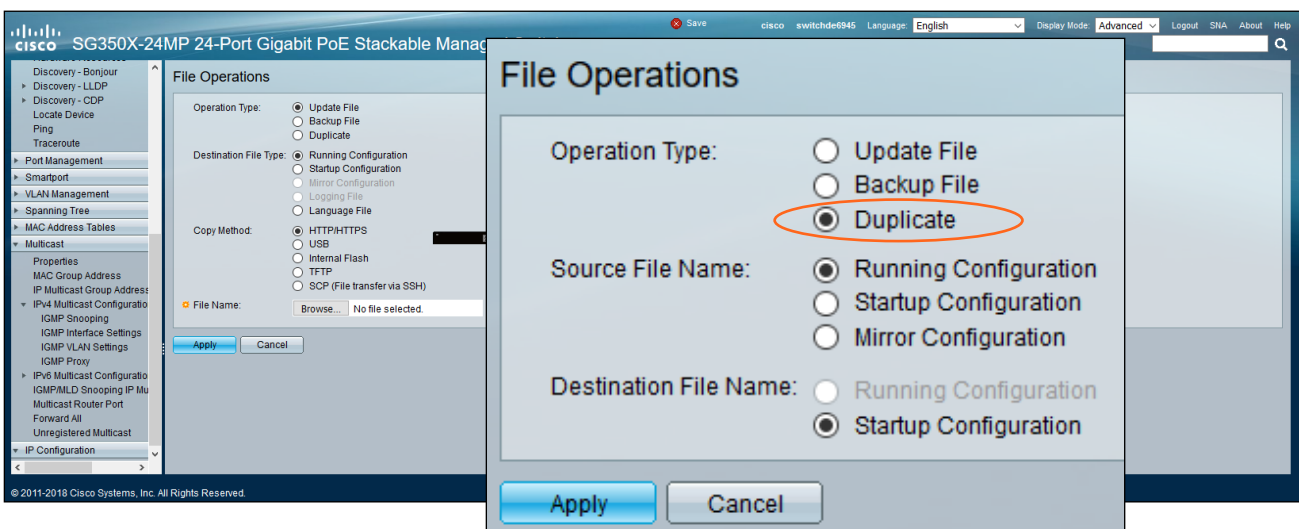
IGMP Querier Status:  Enable

IGMP Querier Election:  Enable

IGMP Querier Version:  v2  
 v3

Querier Source IP Address:  Auto  
 User Defined

60. Click the **VLAN ID** drop-down list, and select the next VLAN ID number. Repeat steps 17 and 18 for each VLAN that was created.
61. Click the **Close** button to dismiss the **Edit IGMP Snooping Settings** dialog.
62. Click **Administration > File Operations** in the menu bar on the left side of the screen. The **File Operations** page will be displayed.
63. Click the **Duplicate** radio button, next to **Operation Type**, then click the **Apply** button to commit changes.



cisco SG350X-24MP 24-Port Gigabit PoE Stackable Manager

File Operations

Operation Type:  Duplicate  
 Update File  
 Backup File

Destination File Type:  Running Configuration  
 Startup Configuration  
 Mirror Configuration  
 Logging File  
 Language File

Copy Method:  HTTP/HTTPS  
 USB  
 Internal Flash  
 TFTP  
 SCP (File transfer via SSH)

File Name:  No file selected.

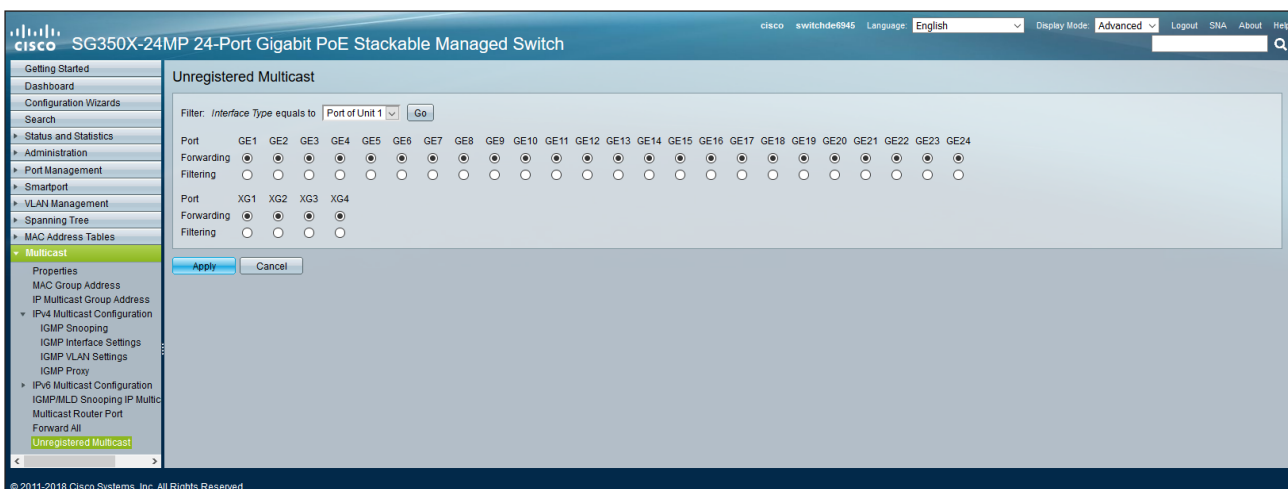
File Operations

Operation Type:  Update File  
 Backup File  
 Duplicate

Source File Name:  Running Configuration  
 Startup Configuration  
 Mirror Configuration

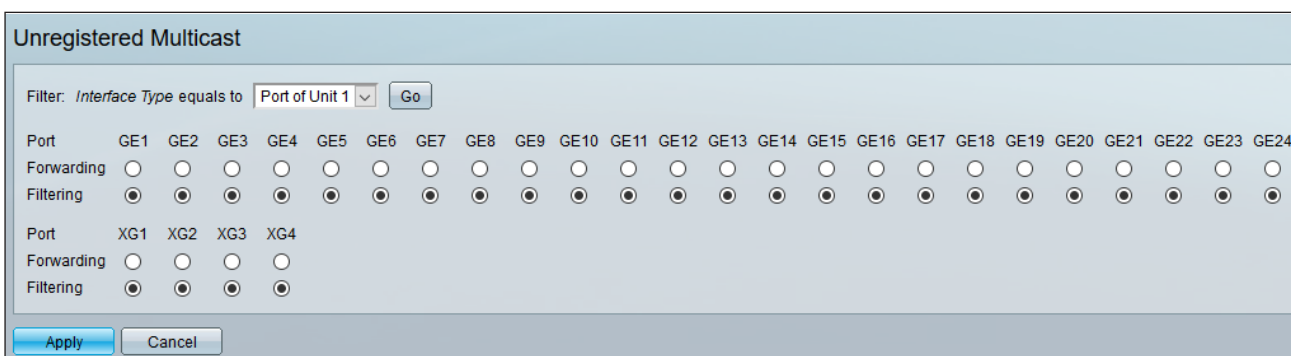
Destination File Name:  Running Configuration  
 Startup Configuration

64. Click **Unregistered Multicast** from the **Multicast** menu on the left side of the screen. By default, all physical ports will have port forwarding enabled, as shown below.



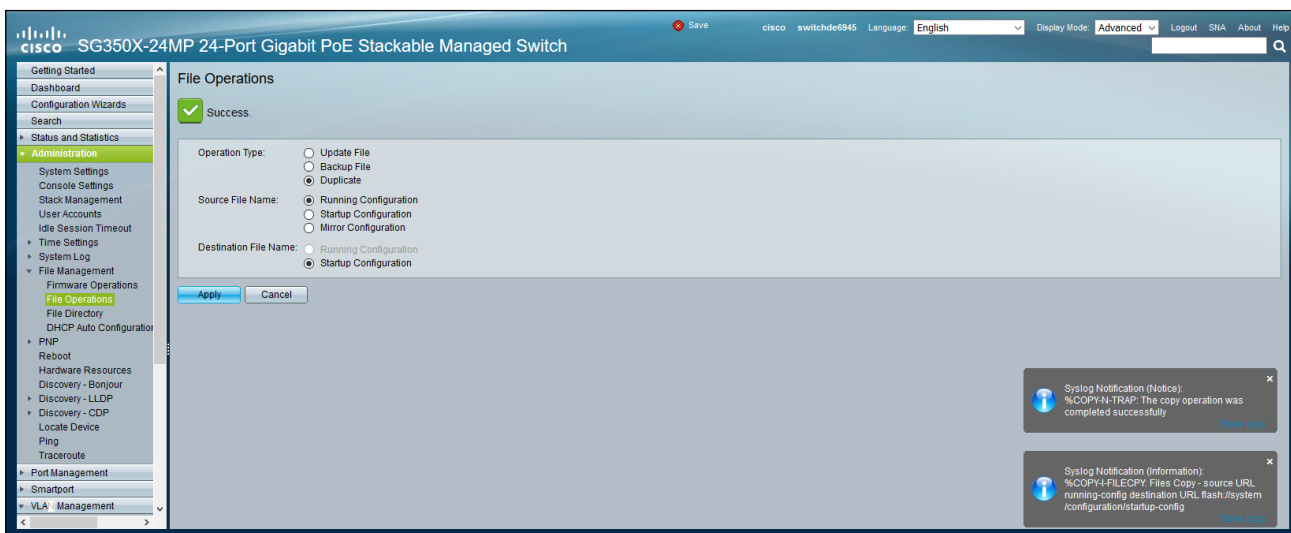
65. Click the **Filtering** radio button to assign port filtering to each port.

66. Click the **Apply** button to commit changes.



67. Click **Administration > File Operations** in the menu bar on the left side of the screen. The **File Operations** page will be displayed.

68. Click the **Duplicate** radio button, next to **Operation Type**, then click the **Apply** button to commit changes.



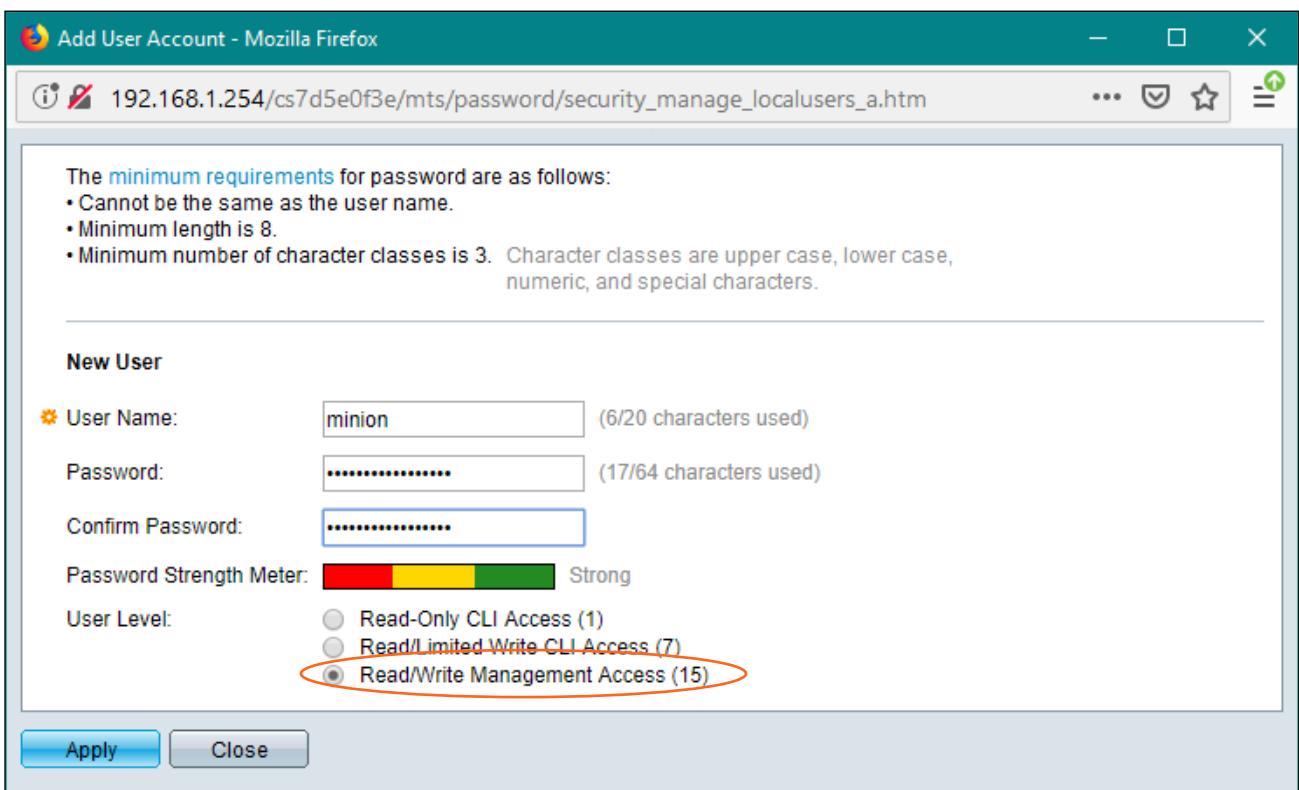
## Creating User Accounts

This next section is optional, and provides instructions on creating user accounts. This is only required if multiple users will need access to the network switch.

1. Click **User Accounts** from the **Administration** menu.



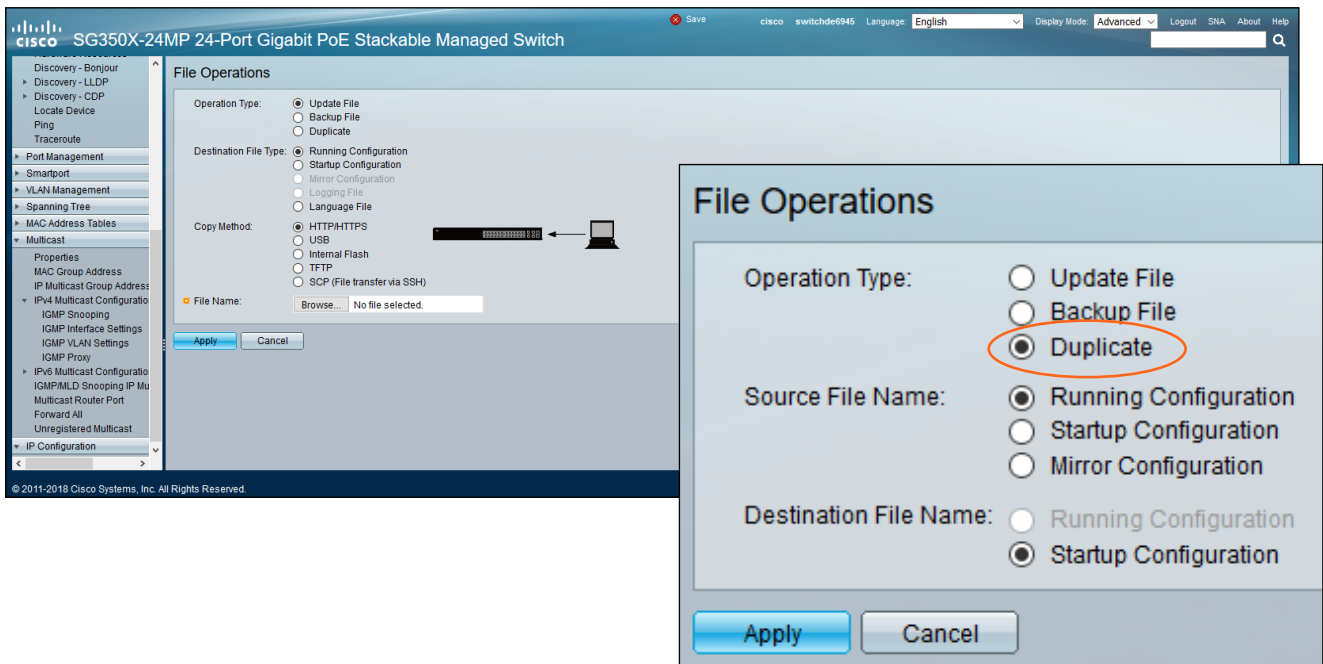
2. Click the **Add...** button to display the **Add User Account** dialog box.
3. Enter the desired username and password in the **User Name** and **Password** fields, respectively. Confirm the password by re-entering it in the **Confirm Password** field.
4. Click the **Read/Write Management Access** radio button, then click the **Apply** button to commit changes.
5. Repeat steps 2 through 4, as required, for each user.
6. Click the **Close** button to dismiss the **Add User Account** dialog box and click **Yes** when prompted to save changes.





## Network Switch Configuration

7. Click **Administration > File Operations** in the menu bar on the left side of the screen. The **File Operations** page will be displayed.
8. Click the **Duplicate** radio button, next to **Operation Type**.
9. Click the **Apply** button to commit changes.
10. Switch configuration is complete.



# Velocity with Integrated AMS

Velocity with Integrated AMS is recommended for configuration of all the OmniStream devices, but before OmniStream is set up, Velocity must be set up and up to date. The following instructions will walk through all the Velocity set up and OmniStream discovery steps.

## Getting an IP Address

### AT-VGW-HW

1. Find the IP of the VGW-HW.
  - a. Using the HDMI port, connect an HDMI cable from the HDMI OUT port to an HDMI IN port on the local display. The unit IP will display at the bottom right hand corner of the display.
  - b. If there is no local display, open the connected PC and do an IP scan using any IP scan program.

### AT-AMS-SW

Follow the installation steps found within the AMS-SW download file. The IP address will be displayed in the Virtual Machine window.

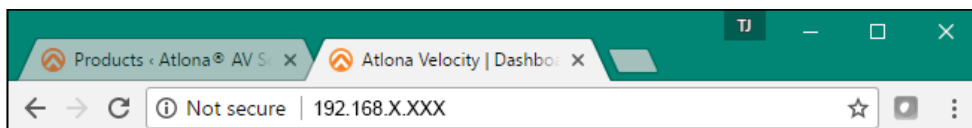
## Login

Once the Velocity Gateway has been set up on a network, locate the IP address of the unit.

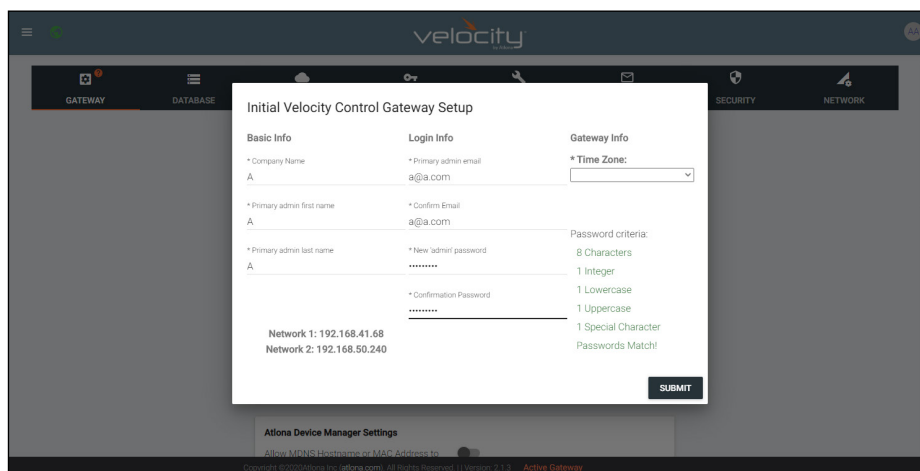
- VGW Hardware: The IP address of the server can be located by connecting to an HDMI or Mini DisplayPort display (the IP will be located on the center of the screen) or using an IP scanner.
- VGW Software: The IP address will be located on the center of the screen after installation.

**NOTE:** Google Chrome is the recommended browser when using Velocity. Other browser may experience technical difficulties and may not support full functionality.

1. Open any browser on the network and type the IP address in, as shown below.



Velocity will automatically log in once the IP is launched and a pop up will appear.



* New 'admin' password	Password criteria:
.....	8 Characters
	1 Integer
* Confirmation Password	1 Lowercase
	1 Uppercase
	1 Special Character
	Passwords do not match.

* New 'admin' password	Password criteria:
.....	8 Characters
	1 Integer
* Confirmation Password	1 Lowercase
	1 Uppercase
	1 Special Character
	Passwords do not match.

* New 'admin' password	Password criteria:
.....	8 Characters
	1 Integer
* Confirmation Password	1 Lowercase
.....	1 Uppercase
	1 Special Character
	Passwords Match!

## Velocity with Integrated AMS

- Fill in the initial set up information, including: Company Name, First & Last name, the email address for system emails to be sent, time zone, and a new password.

**NOTE:** Passwords must be at least 8 characters and include: 1 number, 1 uppercase letter, 1 lowercase letter, and 1 special character. The text will appear all green when the password meets all criteria.

- Press **SUBMIT** once all information is filled. A new pop up will appear.

**NOTE:** Once the initial log in and activation is complete, the new password should be kept somewhere easy to find. If the password is lost, please follow the directions in the **Reset Password** section.

## Updating

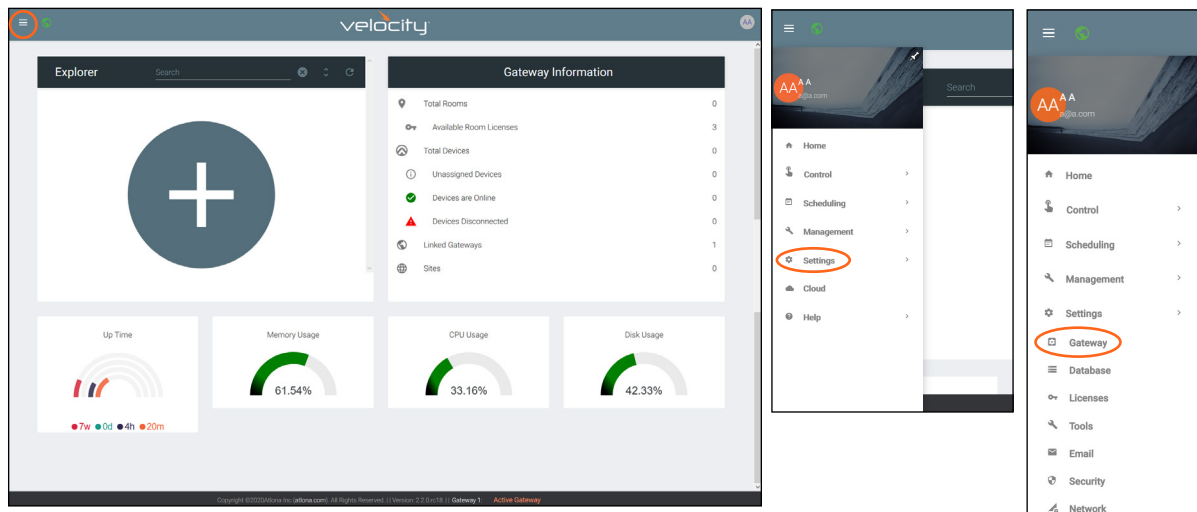
Before discovery, it is best to ensure that Velocity is on the most recent firmware.

If the PC or Velocity are connected to a network with internet connectivity, Velocity will automatically check for updates and give an update notification in the top right corner of the screen if behind. Select the icon and it will go directly to the Firmware tab inside the System Settings. Follow step 4 of the following update instructions.

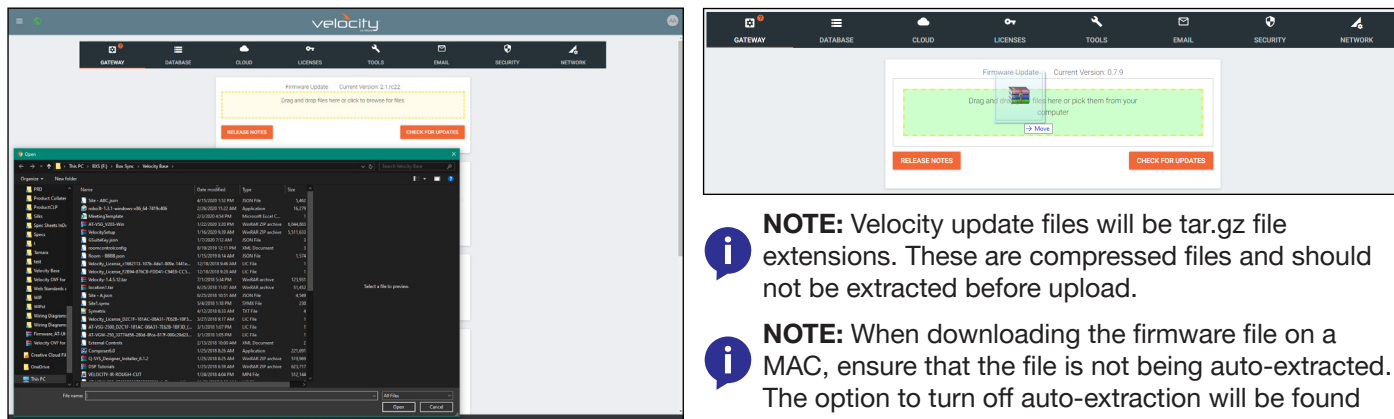


If the PC or Velocity do not have internet connectivity, the firmware can be checked and/or downloaded at <https://atlona.com/product/at-ams-sw/> under the Firmware tab. Velocity's firmware version can be found at the bottom of the main screen. If a manual update is needed, go to the firmware section within Server Settings.

- Locate the ≡ in the top left corner of the home page and left click to open the menu.
- Select **Settings** from the menu. New options will appear.
- Select **Gateway**.



- Click on the field to browse the local computer for the firmware file, or drag and drop the firmware into the field.

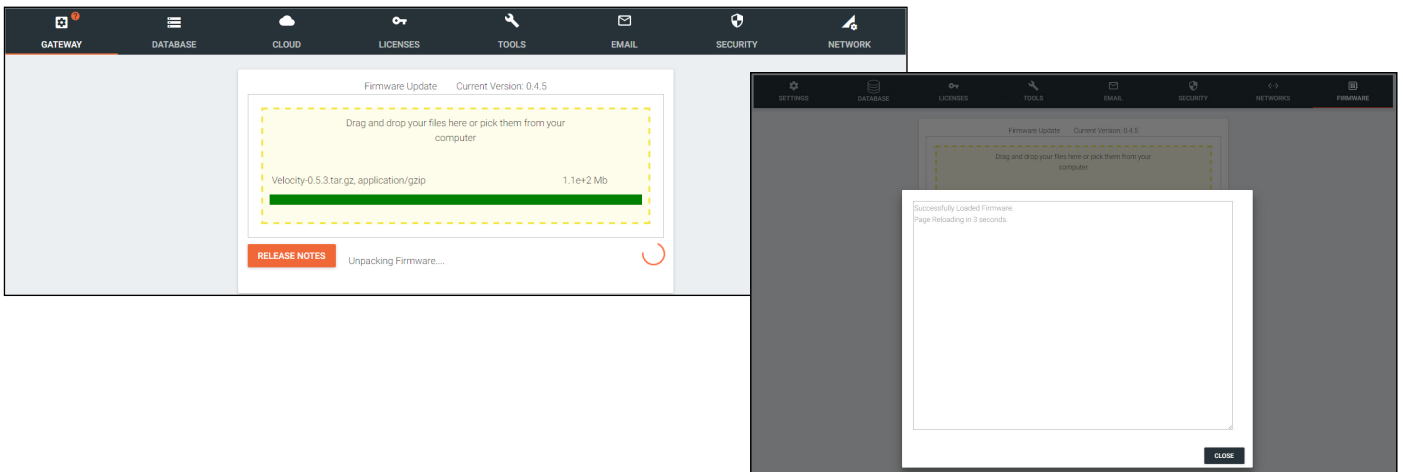


**NOTE:** Velocity update files will be tar.gz file extensions. These are compressed files and should not be extracted before upload.

**NOTE:** When downloading the firmware file on a MAC, ensure that the file is not being auto-extracted. The option to turn off auto-extraction will be found within the browser settings.

## Velocity with Integrated AMS

Firmware upgrading will start automatically.

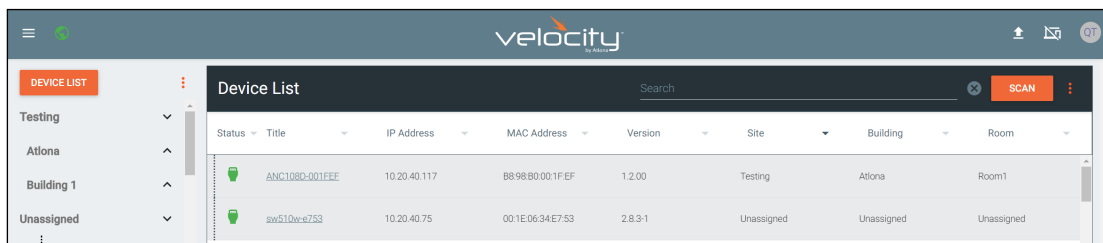
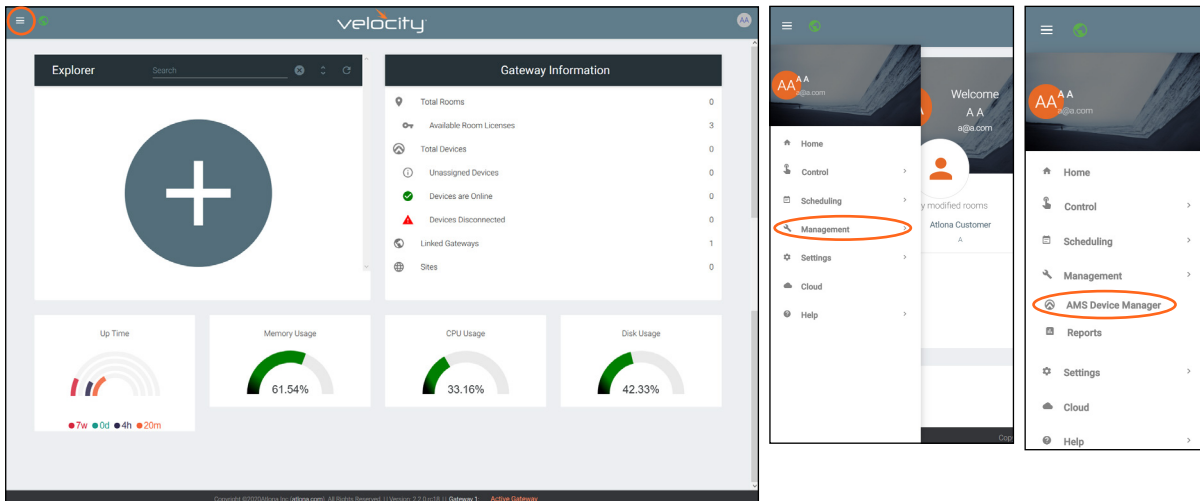


When the firmware upgrade is successfully completed, a pop up window will appear. It will close a few seconds later.

## Discovery

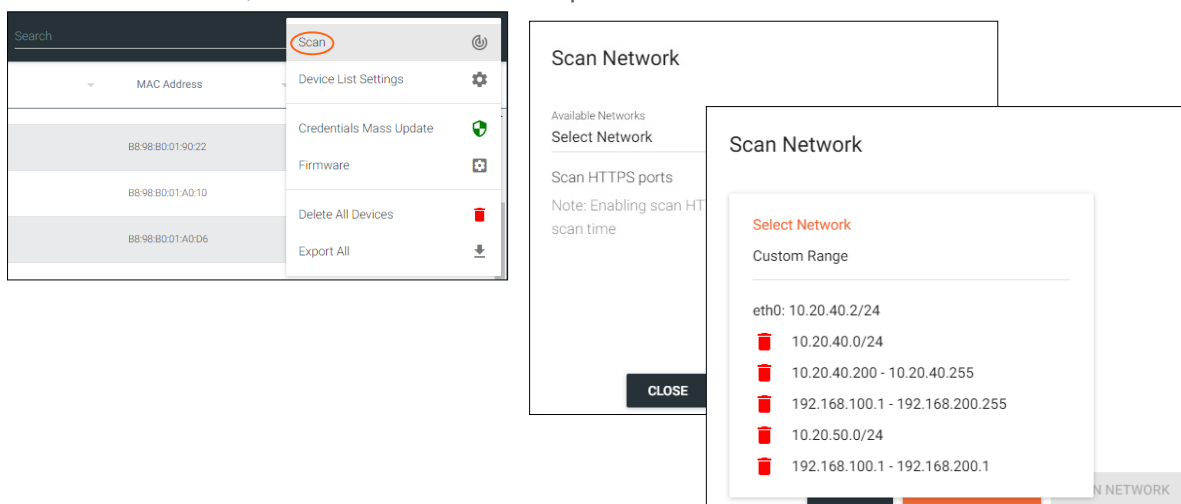
Once Velocity is fully updated, all OmniStream devices can be found through the device list or rooms page. These instructions will provide steps for device list discovery.

1. Locate the ≡ in the top left corner of the home page and left click to open the menu.
2. Select **Management** from the menu. New options will appear.
3. Select **AMS Device Manager**.



OmniStream devices are located through mDNS autoscan and should automatically be discovered and placed under the unassigned list, but if a device isn't listed (or using the AT-OMNI-311 and AT-OMNI-324), use the network scan to find it.

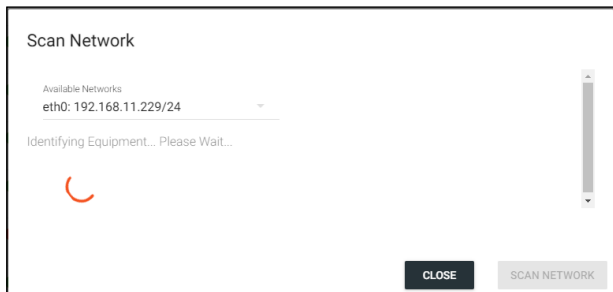
1. Select the **SCAN** button or press the ⋮ icon next to the SCAN button. A new pop up will appear.
  - a. If ⋮ is selected, choose Scan from the drop down menu.



2. Select Custom Range (a new screen will take over) or the auto detected network eth0.

## Velocity with Integrated AMS

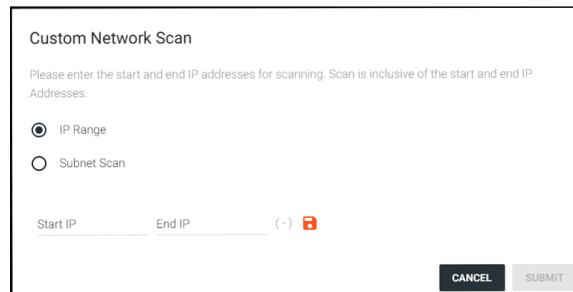
- a. If the auto detected network eth0 is selected, press Scan Network to start the scan.
- b. If Custom Range is selected, select between IP Range and Subnet Scan



**Scan Network**

Available Networks  
eth0: 192.168.11.229/24

Identifying Equipment... Please Wait...



**Custom Network Scan**

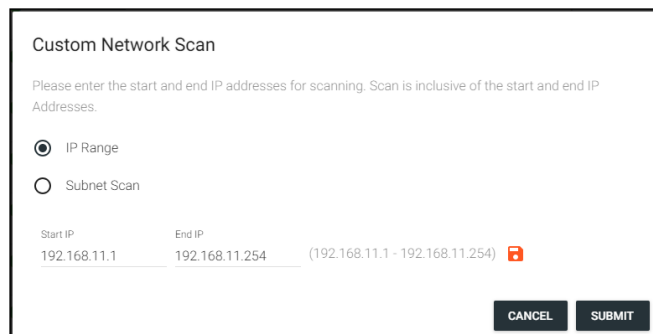
Please enter the start and end IP addresses for scanning. Scan is inclusive of the start and end IP Addresses.

IP Range  
 Subnet Scan

Start IP \_\_\_\_\_ End IP \_\_\_\_\_ (-)

1. Type in the network range or subnet information.

**NOTE:** It is recommended to keep the network range scan to under a 512 IP range. The larger the network range, the longer the scan will take. On subnet scan, AMS will automatically limit the scan to 512 on subnet 23 or 256 on subnet 24.

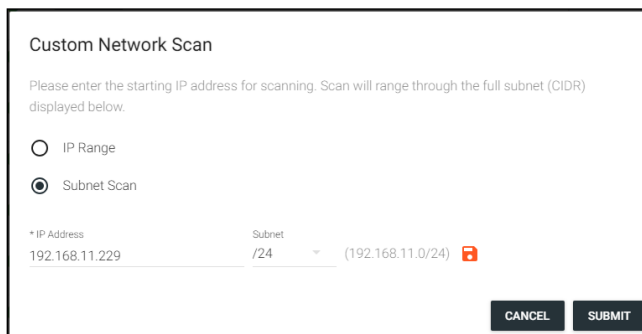


**Custom Network Scan**

Please enter the start and end IP addresses for scanning. Scan is inclusive of the start and end IP Addresses.

IP Range  
 Subnet Scan

Start IP \_\_\_\_\_ End IP \_\_\_\_\_ (192.168.11.1 - 192.168.11.254)



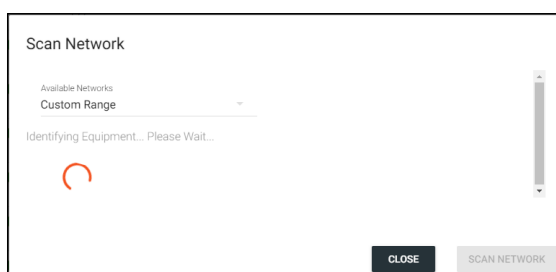
**Custom Network Scan**

Please enter the starting IP address for scanning. Scan will range through the full subnet (CIDR) displayed below.

IP Range  
 Subnet Scan

\*IP Address \_\_\_\_\_ Subnet \_\_\_\_\_ (192.168.11.0/24)

2. Press the save icon next to IP field. A green CustomNetwork Saved Successfully message will appear at the bottom of the page when the custom scan settings are saved. CustomNetwork Saved Successfully. [UNDO](#)
3. Press the Submit button to start the scan. The pop up will close when the scan is completed.




**Scan Network**

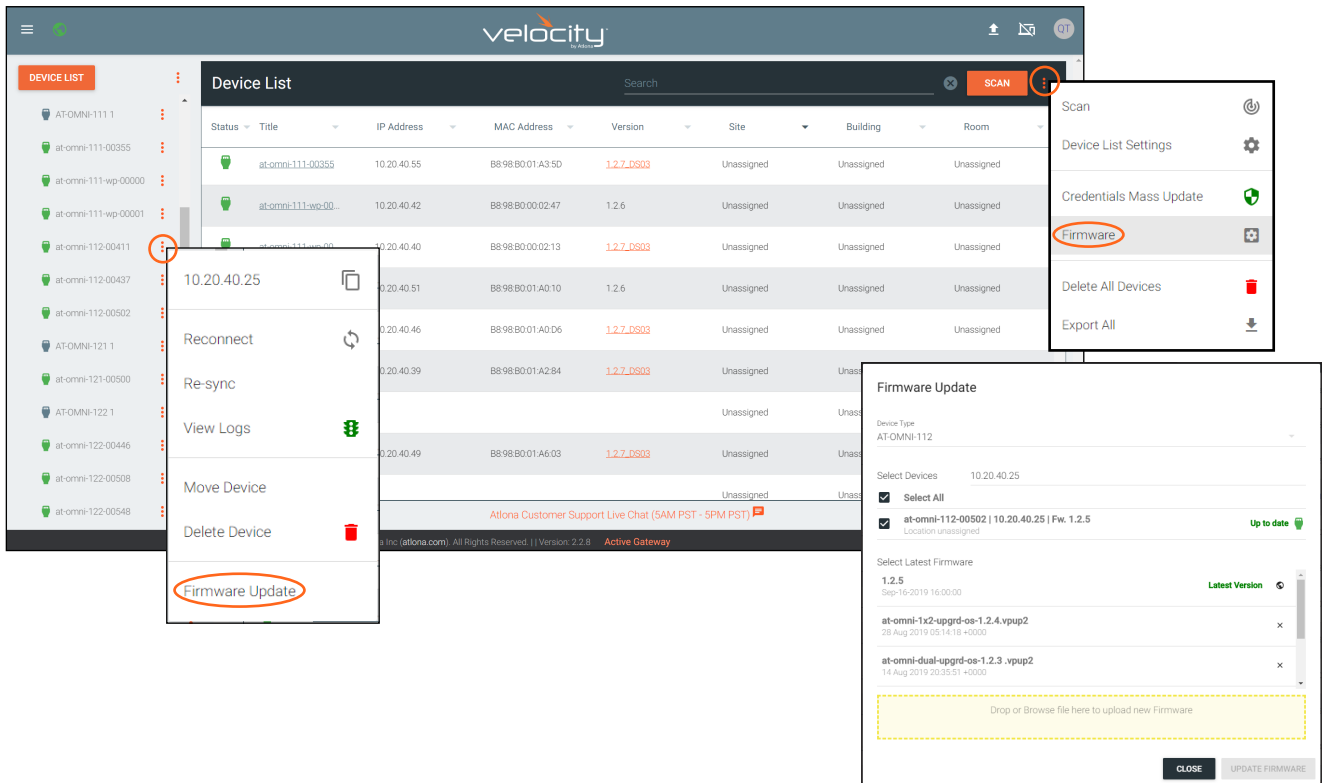
Available Networks  
Custom Range

Identifying Equipment... Please Wait...

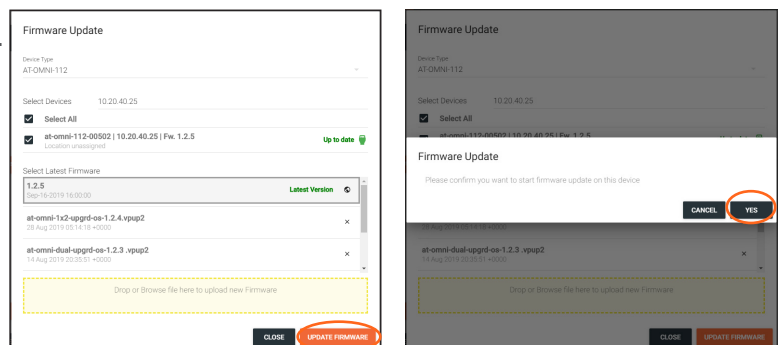
# Updating Device Firmware

Once all devices are discovered, ensure they are the correct firmware. When AMS or the PC connected to AMS is connected to the internet, it will automatically display if an update is needed under the update list or the firmware tab can be checked on <https://atlon.com> for each individual device.

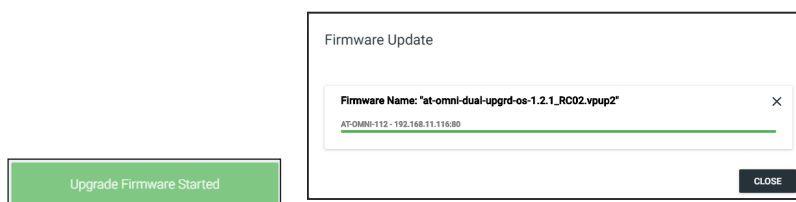
1. Select the  icon within the device list (circled below) or next to the scan button and select Firmware Update from the drop down menu. A new pop up will appear.



2. Drag and drop the firmware from the local PC or select the yellow box to browse the local computer. Once the firmware file has been uploaded, it will appear under the **Select Firmware** section of the dialog box.
3. Select the firmware file name, so that it is highlighted grey.
4. Select **UPDATE FIRMWARE** button to begin the update process, at the bottom of the dialog box.
5. Select **YES** on the confirmation pop up window.



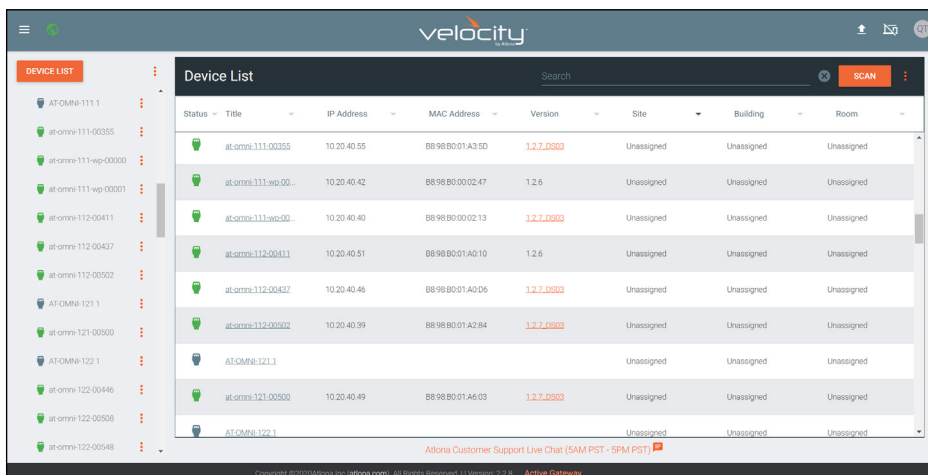
After the **YES** button is clicked, the Upgrade Firmware Started message box will be displayed at the bottom of the page.



The progress bar for the update process will be displayed. The update process should take a few seconds. When done, press the close button and then refresh the browser page. The update is complete.

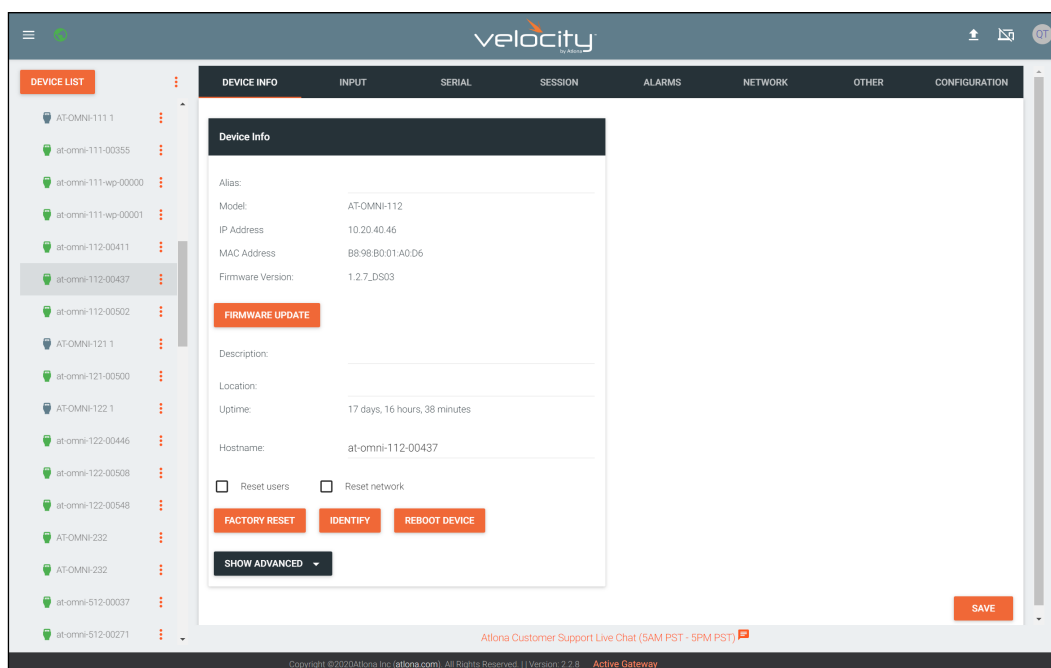
# Configuring OmniStream Devices

Once all devices are up to date, they can be configured.

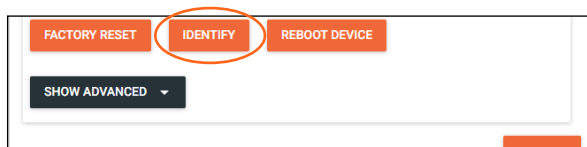


If labeling devices, the IP address can be found on the device list, next to the MAC address. If the MAC address was not noted, the IDENTIFY button can be used within the interface discussed in this section.

1. Select an encoder (AT-OMNI-11X), either from the Unassigned list or the name link in the device list. This will open the encoder’s interface to the Info tab.

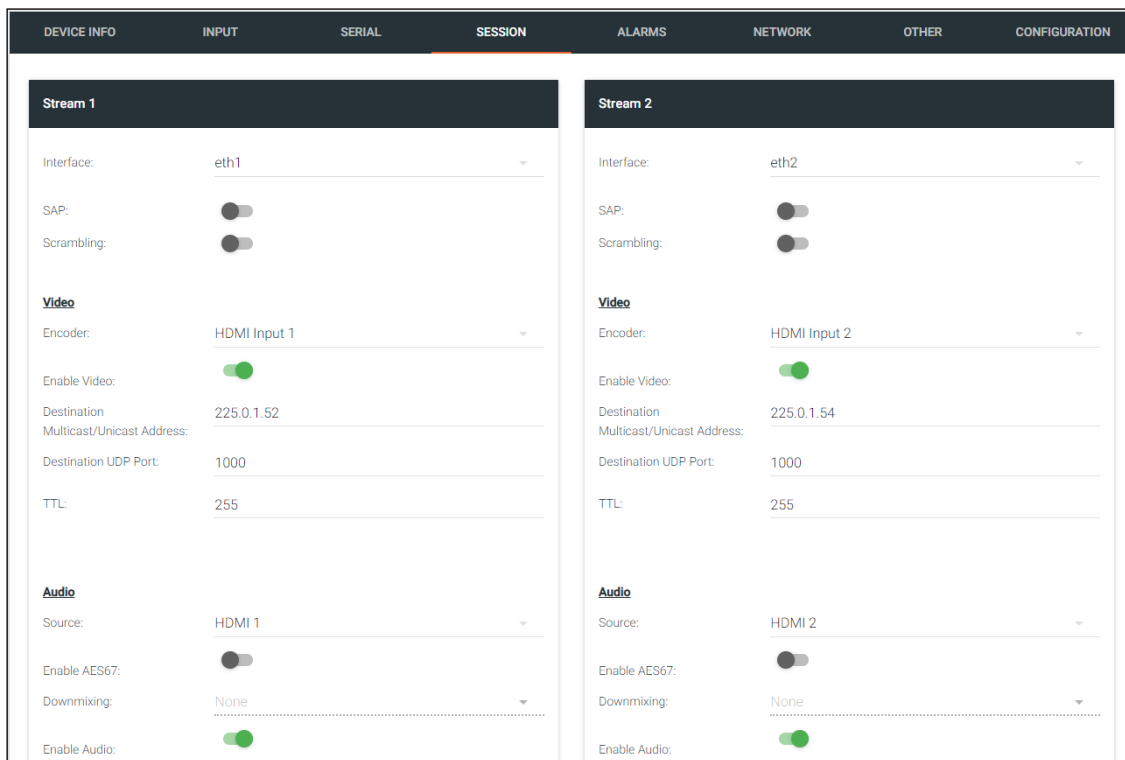


**NOTE:** Scroll to the bottom to find the IDENTIFY button, pressing it will blink the front LEDs of the currently selected OmniStream encoder.



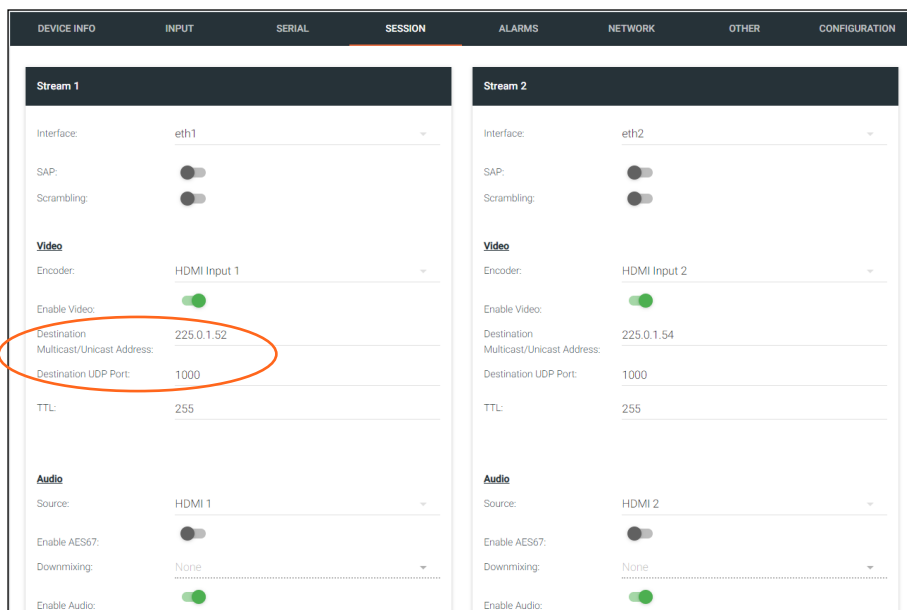


2. Select the Session tab.



The screenshot shows the configuration interface for two streams. The 'SESSION' tab is selected. Stream 1 is configured with interface eth1, SAP and Scrambling toggles off, Video Encoder set to HDMI Input 1, Enable Video checked, Destination Multicast/Unicast Address 225.0.1.52, Destination UDP Port 1000, TTL 255, Audio Source HDMI 1, Enable AES67 off, Downmixing None, and Enable Audio checked. Stream 2 is configured with interface eth2, SAP and Scrambling toggles off, Video Encoder set to HDMI Input 2, Enable Video checked, Destination Multicast/Unicast Address 225.0.1.54, Destination UDP Port 1000, TTL 255, Audio Source HDMI 2, Enable AES67 off, Downmixing None, and Enable Audio checked.

3. For the initial configuration to make sure all things are set up to display audio and video to other devices, only the Destination IP Address and UDP Port fields are required. Scroll down to the Video section first.
4. Velocity will automatically assign an IP address and UDP port, notate the Video IP and Port or if preferred, type in a new multicast IP and Port.



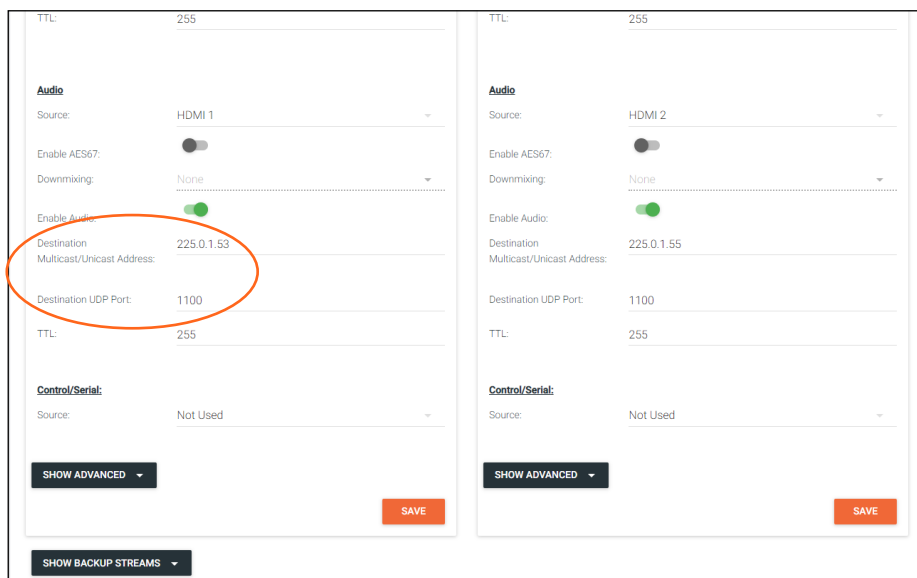
This screenshot is identical to the previous one, but the 'Destination Multicast/Unicast Address' field for Stream 1 (225.0.1.52) is circled in red to highlight it as a required field for initial configuration.

**NOTE:** Start with Session 1 and repeat for all the sessions.

5. OPTIONAL: If the source is HDCP protected, then enable the Scrambling toggle. The toggle will turn green when enabled. Then, specify the scrambling key in the Key field. Both the encoder and decoder must use the same key.

## Configuring OmniStream Devices

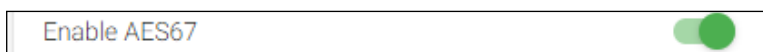
6. Scroll down to the Audio section.
7. Notate the Audio IP and Port or type in a new IP/port. The audio IP and port will differ from the video settings, this allows audio to be routed independently from the video. It is best to have the Destination UDP Port different than the video. So if video is 1000, use 1100 for the audio.



**NOTE:** Start with Session 1 and repeat for all the sessions.

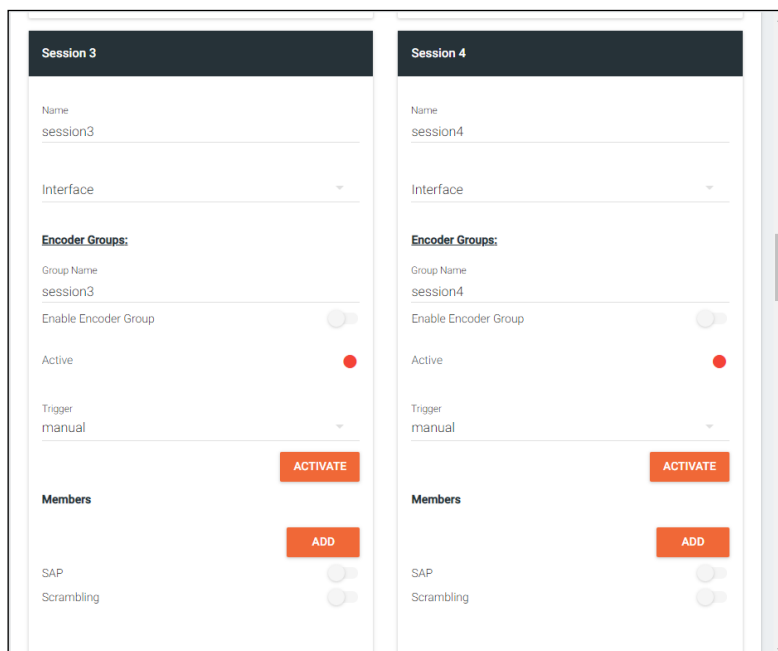
**NOTE:** By default, the AT-OMNI-238 subscribes to streams in the 239.69.0.0/16 subnet.

**NOTE:** If using AES67 audio routing, be sure to select the Enable AES67 slider so that it is green. The AES67 audio stream will use the IP and Port from step 3.



8. Repeat this step for Session 2 if using a dual channel encoder.

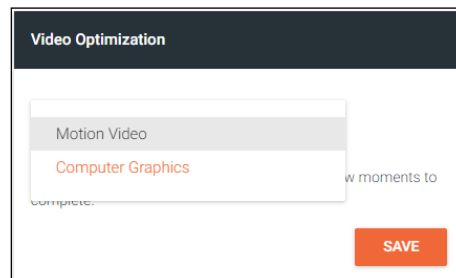
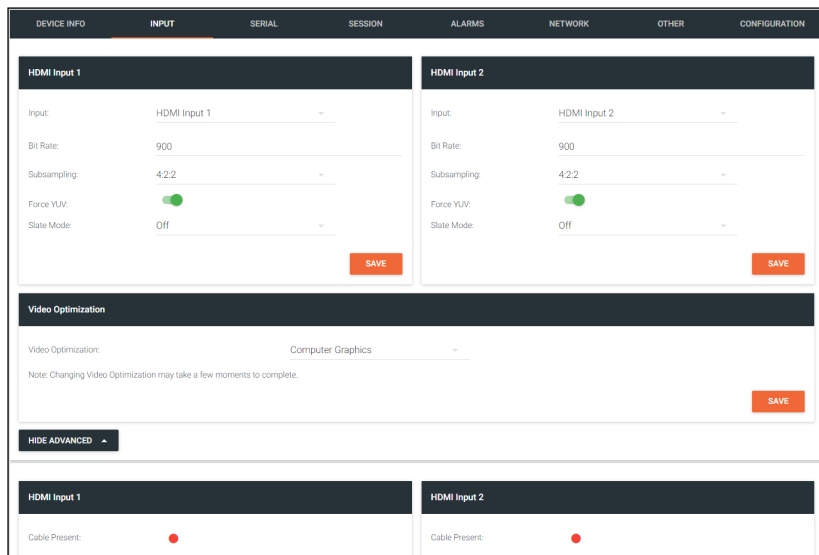
**NOTE:** There will be extra sessions listed on the encoders, these are for redundancy. View the OmniStream manuals to go over redundancy.



## Configuring OmniStream Devices

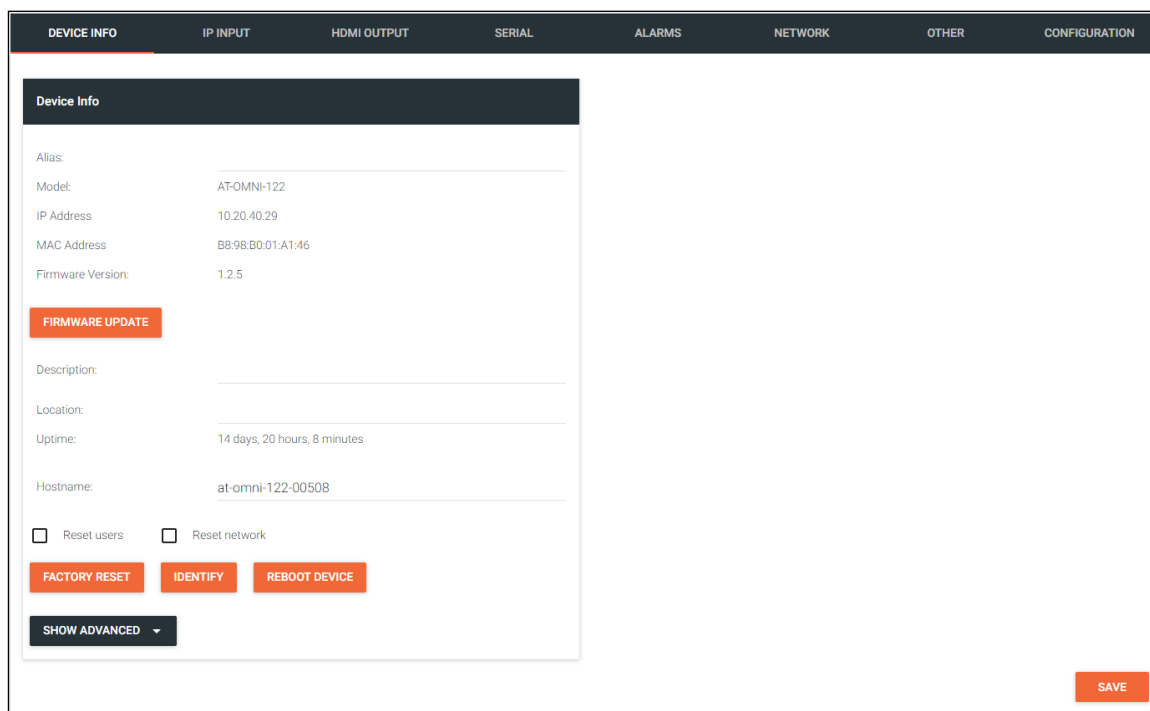
For Pro Series OmniStream only:

With firmware 1.2.2 or greater, Video Optimization can be used. The Video Optimization option must be the same on both the encoder and decoder. For the Encoder this will be found in the INPUT tab.



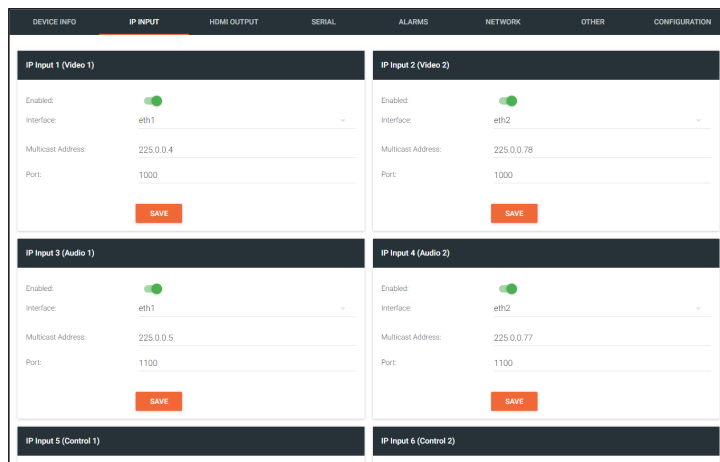
**NOTE:** If connecting a Pro OmniStream series to an R-Type OmniStream, Motion Video must be selected in Video Optimization.

9. Repeat steps 1 through 8 for all encoders.
10. Open a decoder (AT-OMNI-12X).

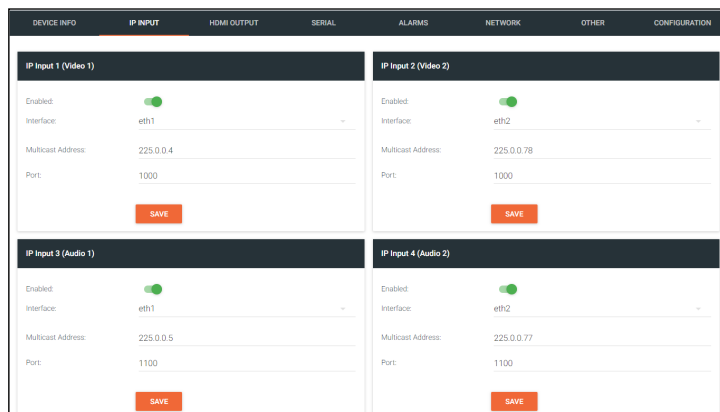


11. Select the IP Input tab.

## Configuring OmniStream Devices

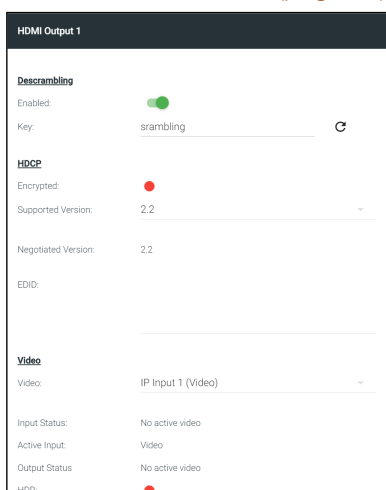
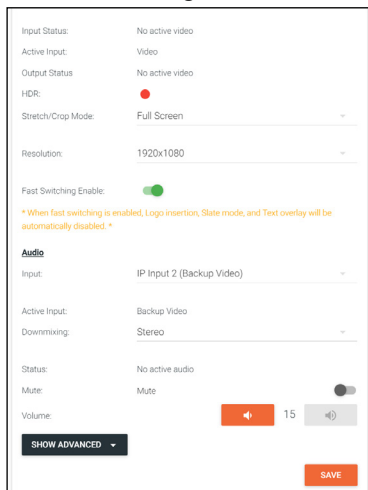
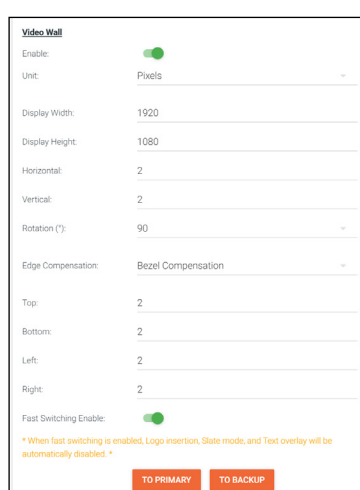


12. Set the Multicast Address to match the video Destination IP and Port from the encoder. **e.g.** Session 1 from the OmniStream 112.
13. Scroll down to Input 3.
14. Enter the IP and Port from the audio source stream to be routed to HDMI OUT 1. **e.g.** Session 3 from the OmniStream 112.



15. Repeat for Session 2 (Video for HDMI OUT 2) and Session 4 (HDMI OUT 2 and analog audio) on the OmniStream dual channel decoders.
16. Repeat steps 10 through 15 for all decoders.

**NOTE:** If the OmniStream devices will be used in a video wall, open the HDMI OUTPUT tab and scroll to the under the Video section and select the slider to enable Video Wall. Select Full Screen from the Stretch/Crop Mode drop down menu under the Video section. No other settings need to be chosen at this time. View the [Video Walls \(page 56\)](#) section for configuration.

# Testing Connectivity

Now that all the OMNIs are set to pass and receive audio and video over IP, basic testing can start.

**NOTE:** Only one source and display are needed for testing, but multiple can be used, to avoid having to disconnect and reconnect the HDMI cable from the OMNIs.

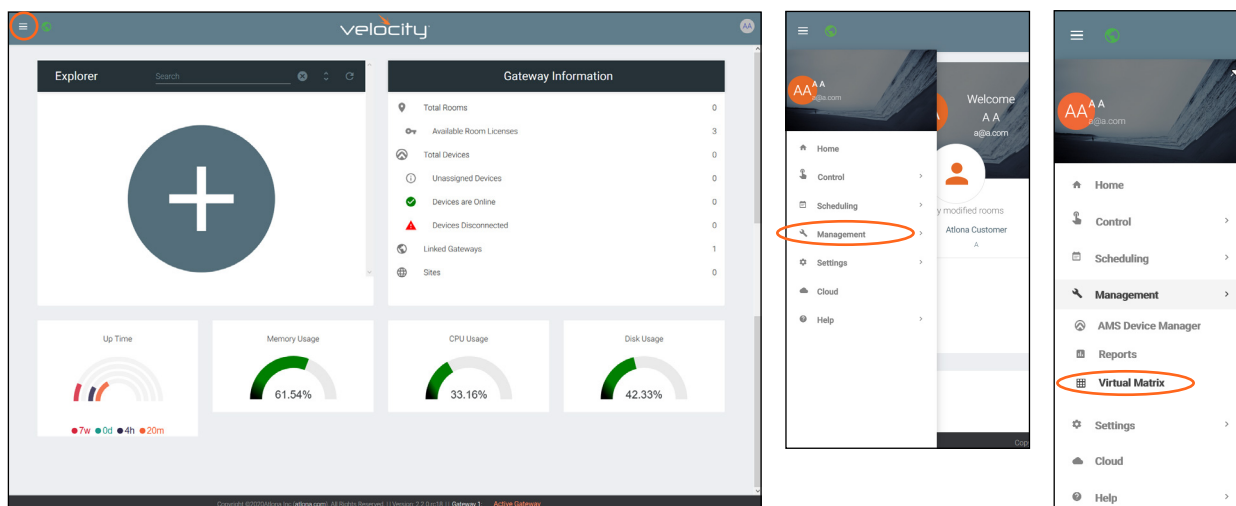
1. Connect the HDMI source to the first encoder port.
2. Connect the HDMI Display to the decoder set up to receive that stream.

If all the streams were set up correctly, audio and video will be passed.

3. Repeat steps 1 and 2 for all encoder and decoder ports.

The Audio / Video Settings section can be used to adjust video input and output resolutions and settings for each stream. View the OmniStream manuals for more information.

4. OPTIONAL: Test routing and ensure connectivity with all the units using the Virtual Matrix.
  - a. Locate the ≡ in the top left corner of the home page and left click to open the menu.
  - b. Select **Management** from the menu. New options will appear.
  - c. Select **Virtual Matrix**.



- d. To route audio and video in one press select the square that corresponds with the port and device to test. Repeat until all units have been tested.

Encoders / Decoders		LEGEND	AT-OMNI-121 1	AT-OMNI-521 1
Video	View: Active		Disconnected	Disconnected
Audio	All		Options	
Data	Flip Matrix		HDMI 1 Out	HDMI 1 Out
AT-OMNI-112 1	HDMI 1 In			
Disconnected	HDMI 2 In			
AT-OMNI-512 1	HDMI 1 In			
Disconnected	HDMI 2 In			
AT-OMNI-111 1	HDMI 1 In			
Disconnected				

Encoders / Decoders		LEGEND	AT-OMNI-121 1	AT-OMNI-521 1
Video	View: Active		Disconnected	Disconnected
Audio	All		Options	
Data	Flip Matrix		HDMI 1 Out	HDMI 1 Out
AT-OMNI-112 1	HDMI 1 In			
Disconnected	HDMI 2 In			
AT-OMNI-512 1	HDMI 1 In			
Disconnected	HDMI 2 In			
AT-OMNI-111 1	HDMI 1 In			
Disconnected				

- e. To route audio and video separately, select the audio and video icon at the top left to have the routes display the individual streams under the devices.
- f. Select each icon to switch the audio and video streams until all streams have been tested.

# IR Control

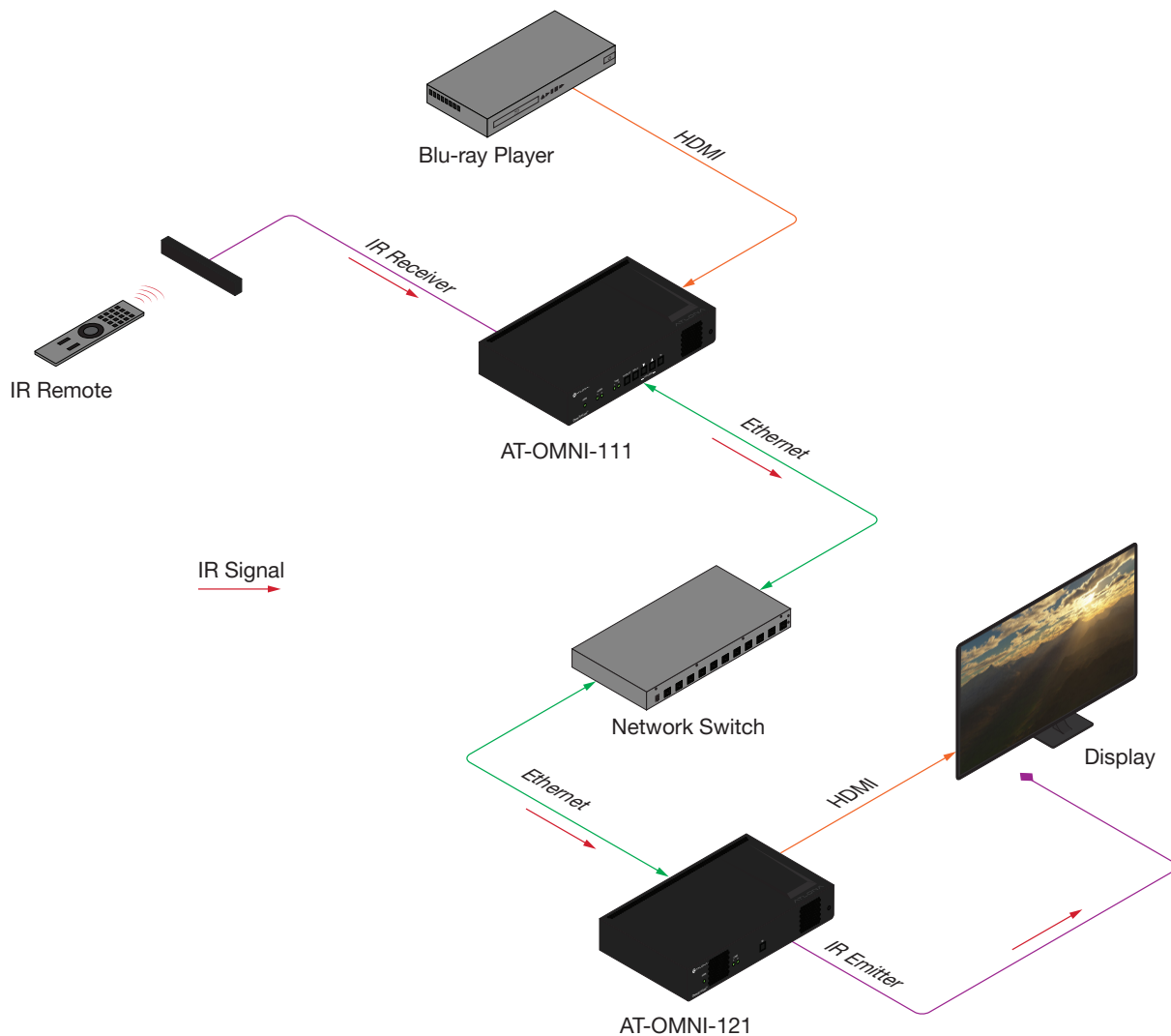
## Controlling the Display using the Display's IR Remote

The same port that provides RS-232 connections also supports bidirectional IR pass-through, allowing a device to be controlled from either the headend or the decoder endpoint. This step is optional. IR control is only supported on **RS-232 2** port (bottom set of connectors).

The following sections provide step-by-step instructions for the following topics:

- Controlling the Display using the Display's IR Remote
- Controlling the Display using a Control System

The illustration below shows a display device being controlled from the encoder. Refer to the next page for details on how to connect the IR emitter and IR receiver.



## Required Equipment

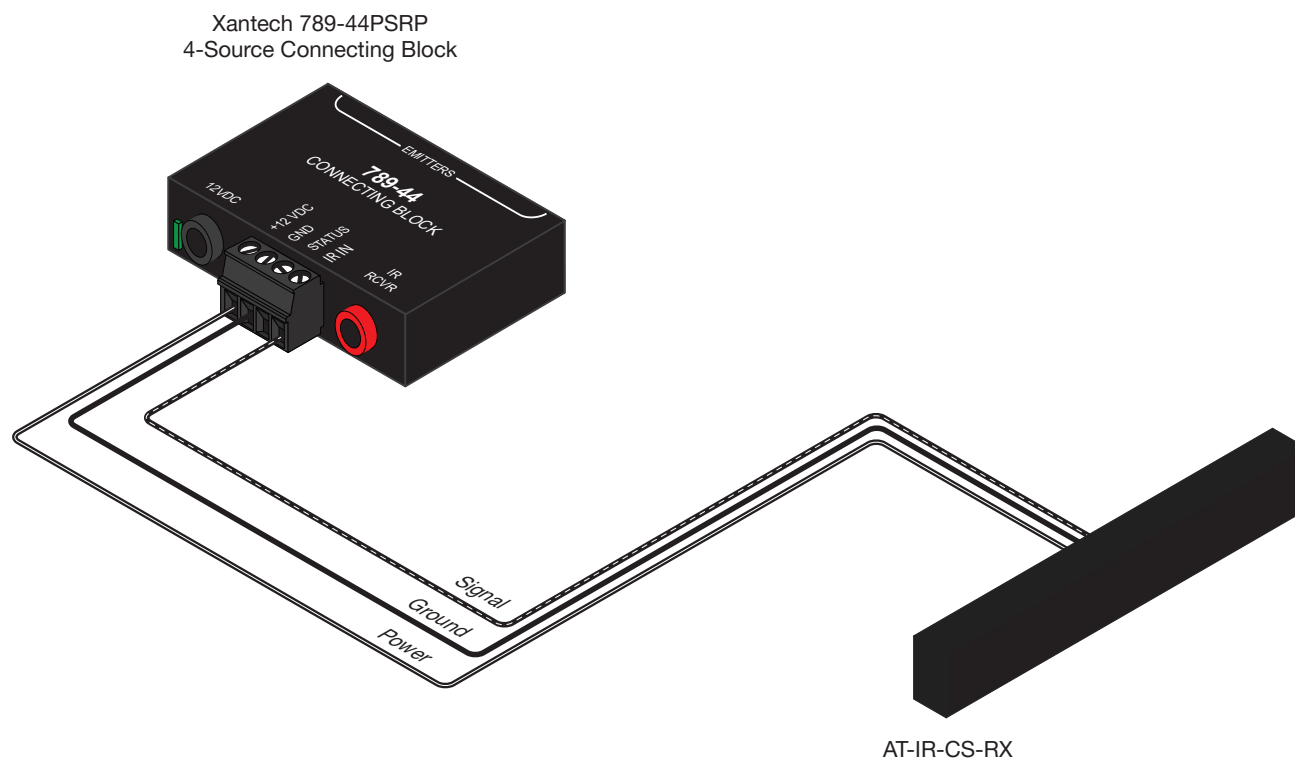
Atlona has tested and verified the following components for this application. However, other components may also be used. Note that IR control is only supported on **RS-232 2** port (bottom set of connectors) of the OmniStream encoder and decoder.

- Xantech 789-44 4-Source Connecting Block
- Xantech 12 V PSU
- IR Receiver (Atlona AT-IR-CS-RX)
- IR Emitter (Atlona AT-OMNI-IR-TX)

## Connecting the IR Receiver to the Encoder

1. Unscrew the captive screw connectors on the Xantech 789-44 4-Source Connecting Block, using a regular screwdriver, and connect the SIGNAL, GROUND, and POWER leads of the AT-IR-CS-RX to the Xantech 789-44 4-Source Connecting Block, as shown below. The presence or absence of white markings on each wire of the AT-IR-CS-RX will denote the signal type:

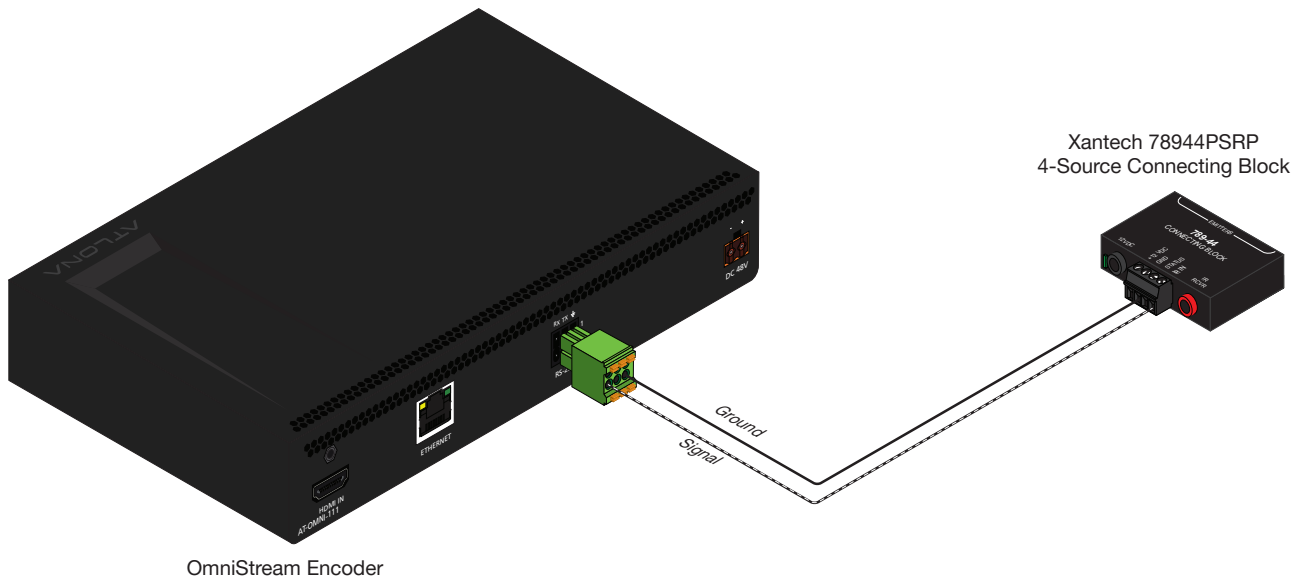
IR IN	= Dashed dark gray line
GND	= Solid (no marking) black wire
+12 VDC	= solid dark gray line



2. Connect the IR IN and GND leads, from the 789-44 4-Source Connecting Block, to the **RX** and  $\perp$  pins, respectively, of the **RS-232 2** port (bottom port) of the encoder, as shown.



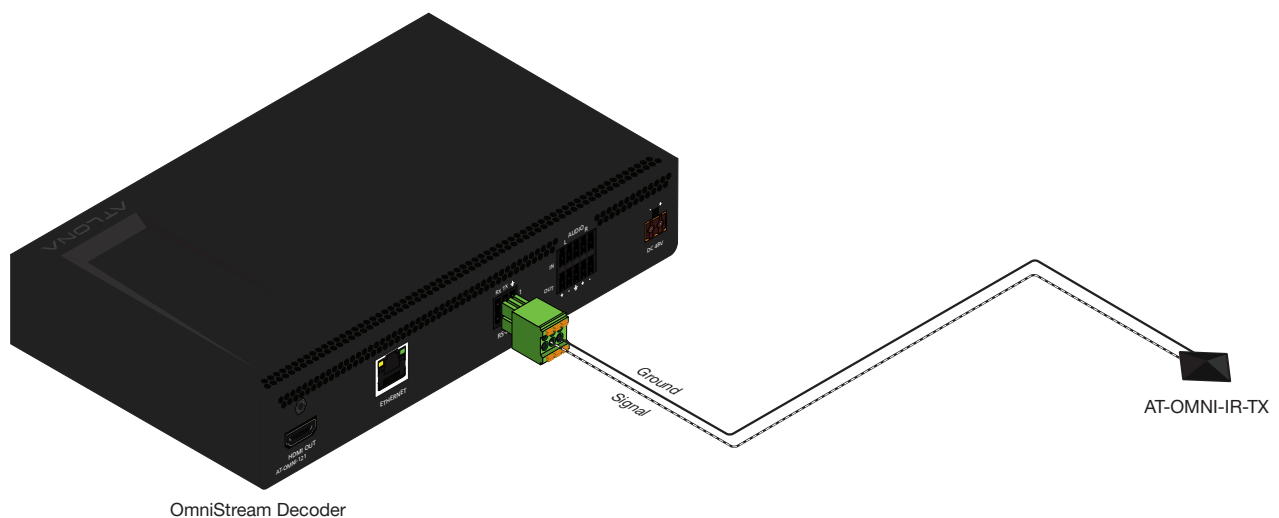
**NOTE:** The IR IN, GND, and +12 VDC wires, from Step 1, have been removed from the illustration below, for purposes of clarity.



3. Connect the Xantech 12 V power supply (or other compatible 12 V DC power supply) to the 12VDC connector on the Xantech 789-44 4-Source Connecting Block.

### Connecting the IR Emitter to the Decoder

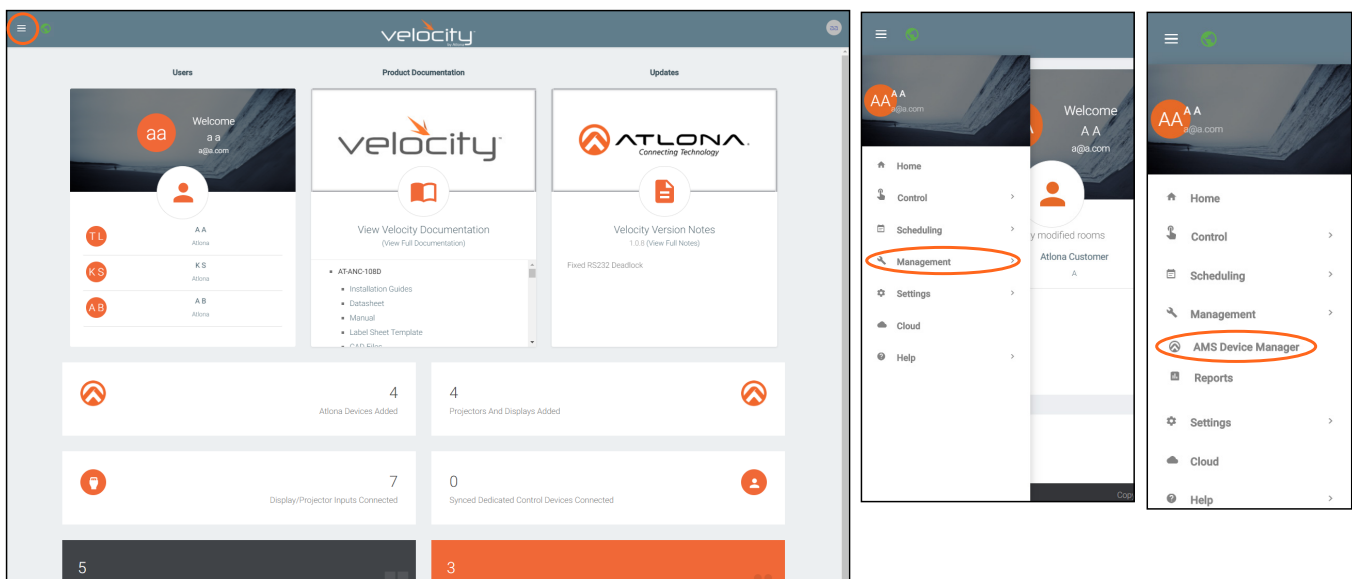
1. Connect the included 6-pin Phoenix connector to the **RS-232 2** port on the encoder.
2. Connect the SIGNAL wire of the AT-OMNI-IR-TX, to the **TX** (middle) terminal on the **RS-232 2** port.
3. Connect the GROUND wire of the AT-OMNI-IR-TX to the  $\perp$  terminal on the **RS-232 2** port.





## Identifying the Encoder using Velocity with Integrated AMS

1. Launch a web browser and enter the IP address of Velocity in the address bar.
2. Enter the required login credentials. The default login is:  
 Username: admin  
 Password: Atlona
3. Click the **Login** button.
4. The Velocity Dashboard will be displayed.
5. Click the = icon, in the upper-left corner of the screen.



6. Select **Management** from the menu.
7. Select **AMS Device Manager**.



8. Click the desired encoder within the **Device List** window. The Velocity interface for the encoder will be displayed.
9. Locate and make note of the IP address of the encoder, which can be found in the **IP Address** field. If using dual-channel encoders, use the IP address in the **IP Address 1** field.

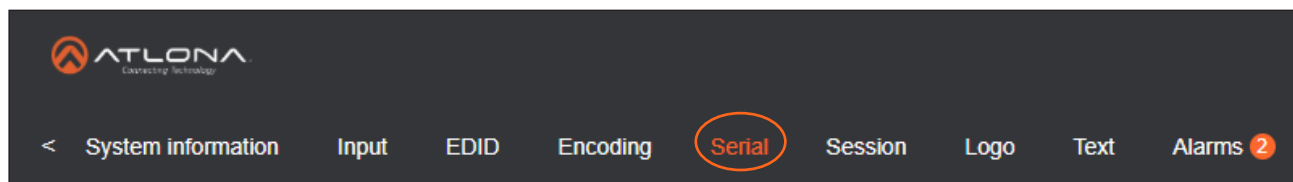
## Configuring the Encoder Serial Port

The first step will be to configure the RS-232 port on the encoder to use IR. Only the **RS-232 2** port supports both RS-232 and IR. Therefore, this port must be used for IR. RS-232 port configuration is managed under the Serial page of the encoder web interface.

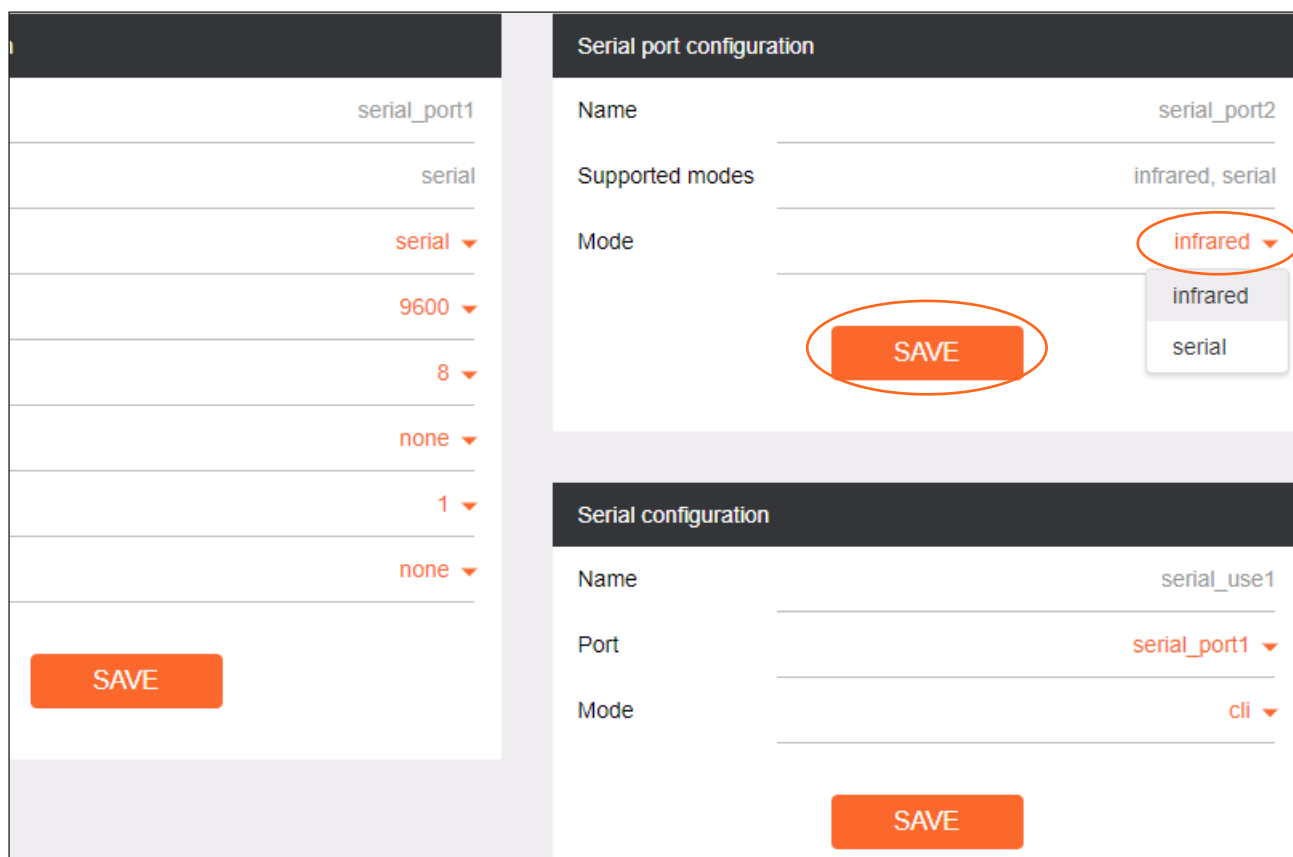
1. Enter the IP address of the encoder in the address bar of the web browser.
2. Enter the required login credentials. The default login is:

Username: admin  
 Password: Atlona

3. Click the **Login** button.
4. Click **Serial** in the top menu bar.



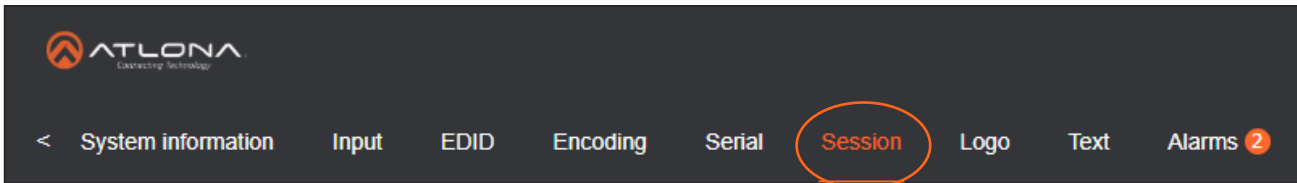
5. Under **Serial Configuration** for serial\_use2, set the port to **Not used**.
6. Locate the **Serial port configuration** window group. The **Name** field, within this window group, should read **serial\_port2**. Click the **Mode** drop-down list and select **Infrared**.
7. Click the **SAVE** button to commit changes.



## Configuring the Encoder Session

The next step is to assign the IR control for Serial Port 2 to the desired Session.

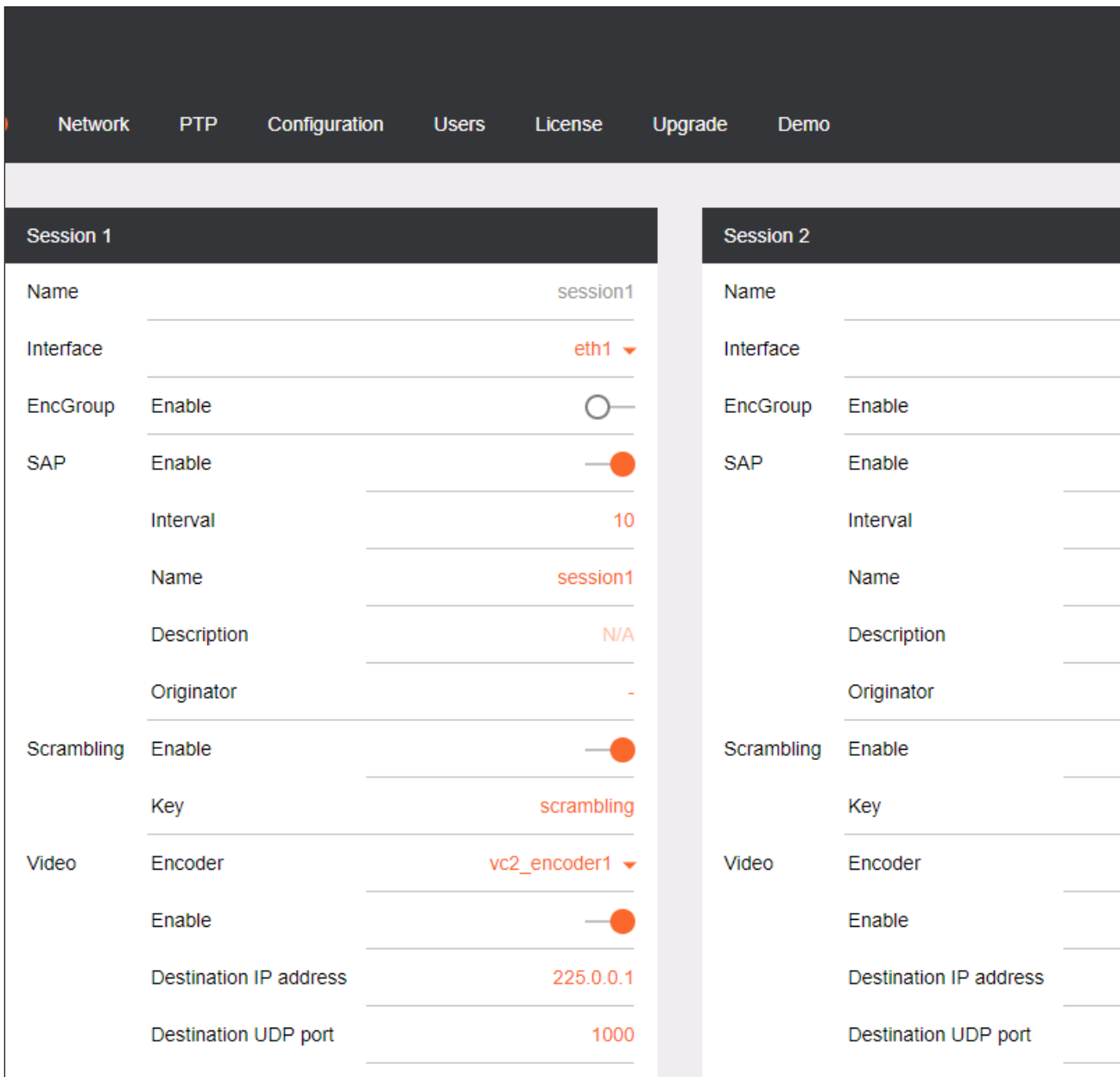
1. Click **SESSION** in the top menu bar.



2. Locate the **Session 1** window group.

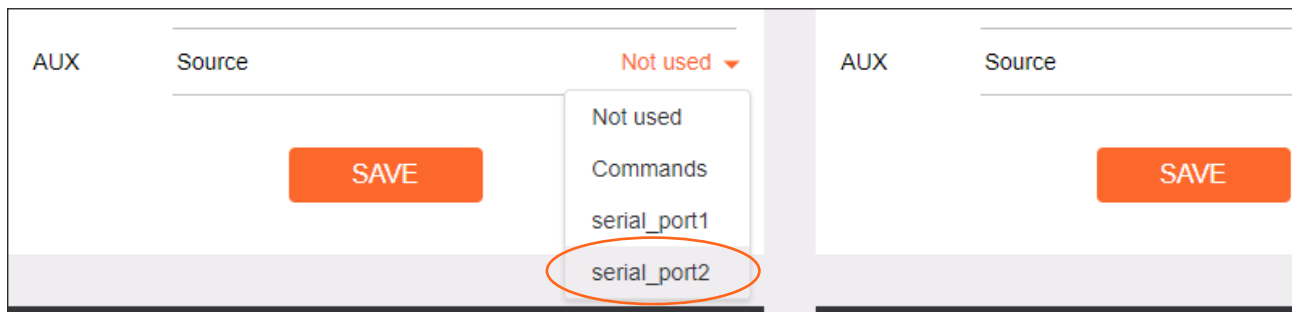


**NOTE:** **Session 2** can also be used with IR. However, in this example, **Session 1** will be configured.

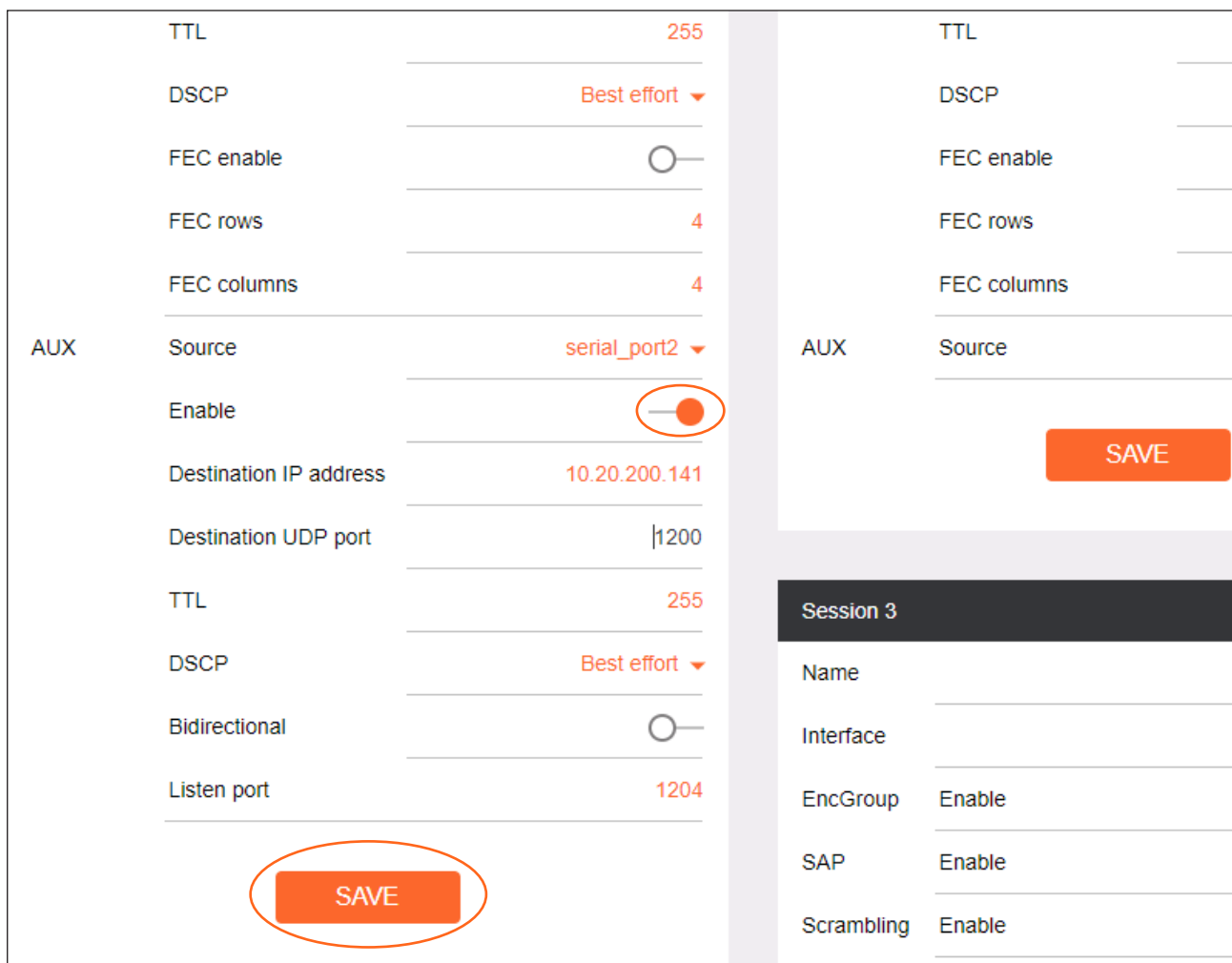


Session 1		Session 2	
Name	session1	Name	
Interface	eth1	Interface	
EncGroup	Enable <input type="checkbox"/>	EncGroup	Enable
SAP	Enable <input checked="" type="checkbox"/>	SAP	Enable
Interval	10	Interval	
Name	session1	Name	
Description	N/A	Description	
Originator	-	Originator	
Scrambling	Enable <input checked="" type="checkbox"/>	Scrambling	Enable
Key	scrambling	Key	
Video	Encoder	Video	Encoder
Encoder	vc2_encoder1	Encoder	
Enable	<input checked="" type="checkbox"/>	Enable	
Destination IP address	225.0.0.1	Destination IP address	
Destination UDP port	1000	Destination UDP port	

3. Scroll down and locate the **AUX** section.
4. Click the **Source** drop-down list and select **serial\_port2**.



5. Enable the auxiliary (AUX) channel by clicking the **Enable** toggle switch. When the auxiliary channel is enabled, this toggle switch will be orange.
6. Enter the IP address of the *decoder* in the **Destination IP Address** field. This is the decoder to which the IR emitter is connected. In this example, the decoder IP address is 10.20.200.141.
7. Enter the port number in the **Destination UDP Port** field.
8. Click the **SAVE** button to commit changes.

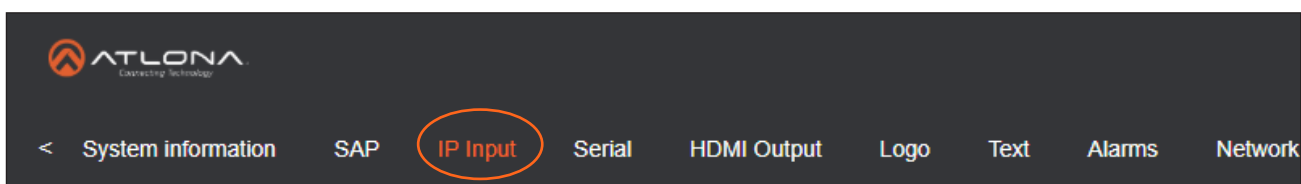


### Configuring the Decoder Serial Port


1. Select the desired decoder within the **AMS Device List** window and make note of the decoder IP address.
2. Enter the required login credentials. The default login is:

Username: admin  
 Password: Atlona

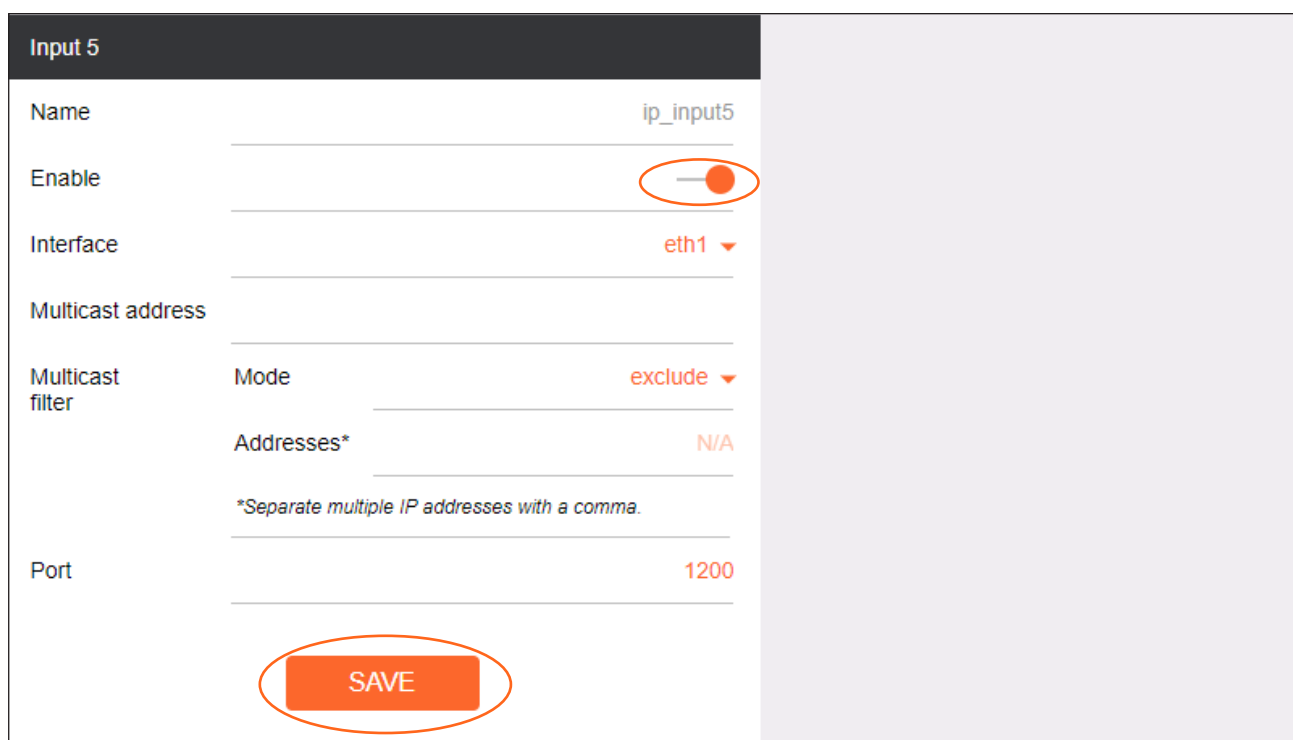
3. Click the **Login** button, then click **IP Input** in the top menu bar.



4. Scroll down to the **Input 5** window group.
5. Enable **Input 5** by clicking the **Enable** toggle switch. When enabled, this toggle switch will be orange.
6. Enter the port in the **Port** field. This port number must be the same port used by the encoder, and is the input of the decoder that will receive IR data.

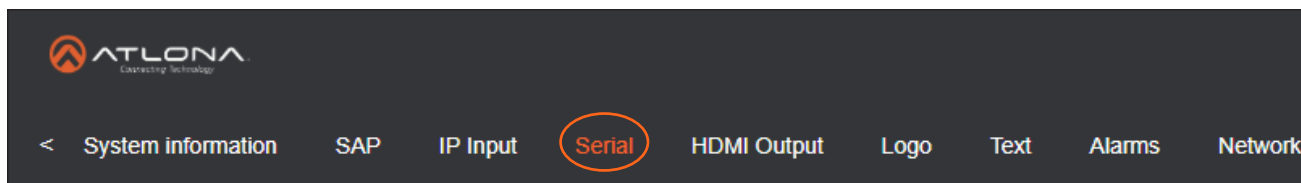
 **IMPORTANT:** Do not change the contents of the **Multicast Address** field. This field should be left blank if using unicast IR.

7. Click the **SAVE** button to commit changes.



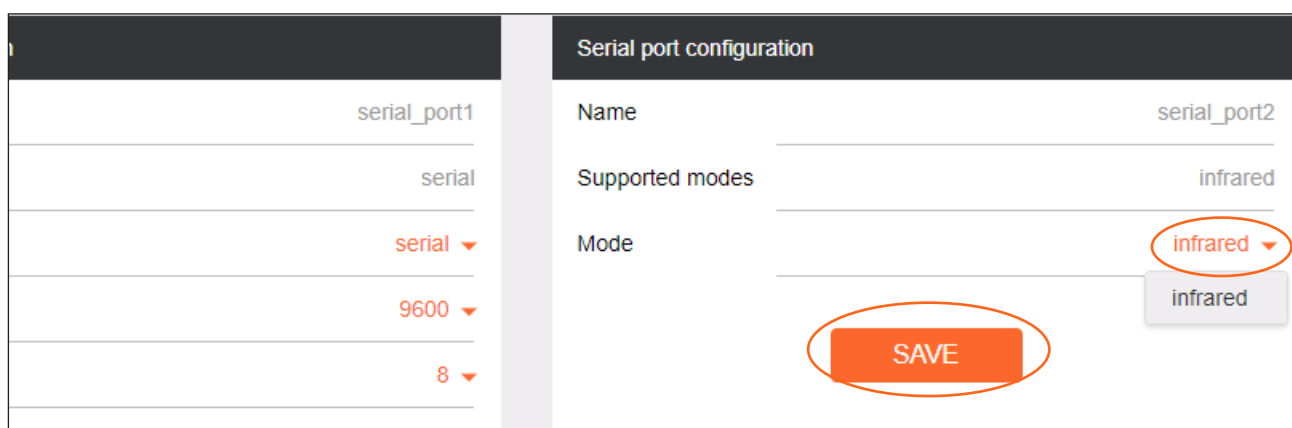
Input 5	
Name	ip_input5
Enable	<input checked="" type="checkbox"/>
Interface	eth1 ▼
Multicast address	
Multicast filter	Mode: exclude ▼
	Addresses*: N/A
<small>*Separate multiple IP addresses with a comma.</small>	
Port	1200
<b>SAVE</b>	

8. Click **Serial** in the top menu bar.



9. Locate the **Serial port configuration** window group. The **Name** field, within this group, should read **serial\_port2**. Click the **Modes** drop-down list and select **Infrared**.

10. Click the **SAVE** button to commit changes.

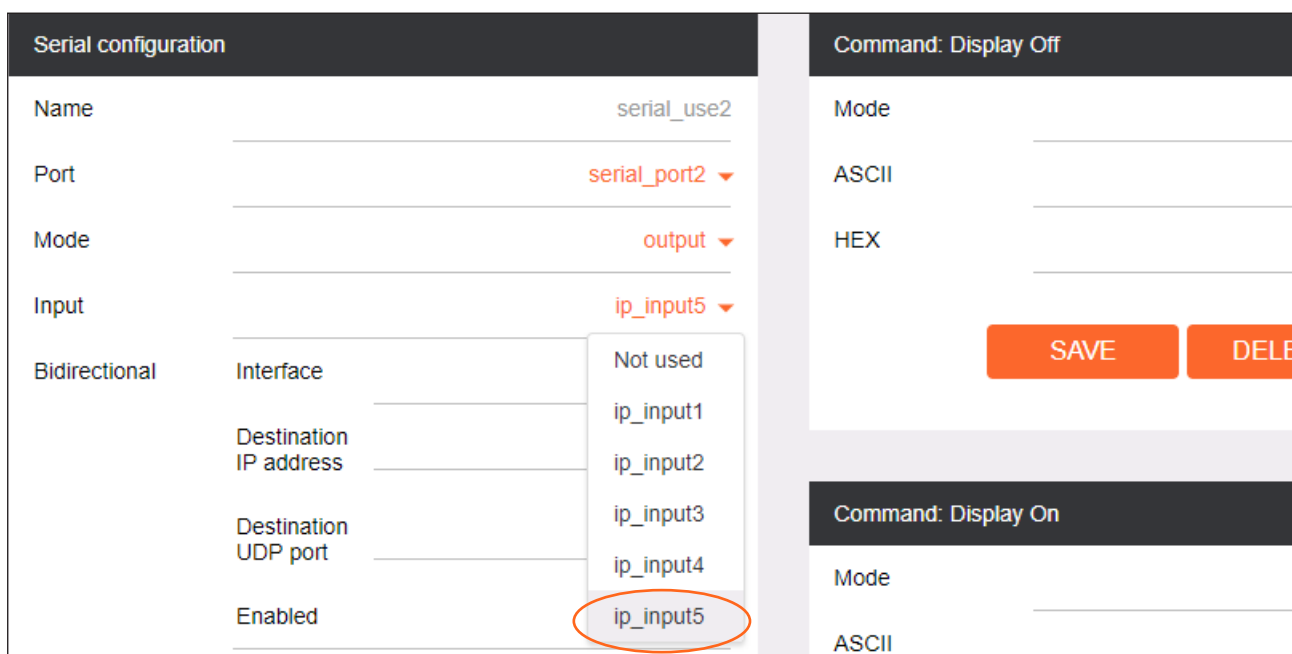


11. Scroll down the page and locate the **Serial Configuration** window group. The **Name** field, within this group, should read **serial\_use2**.

12. Click the **Port** drop-down list and select **serial\_port2**.

13. Click the **Mode** drop-down list and select **output**.

14. Click the **Input** drop-down list and select **ip\_input5**.




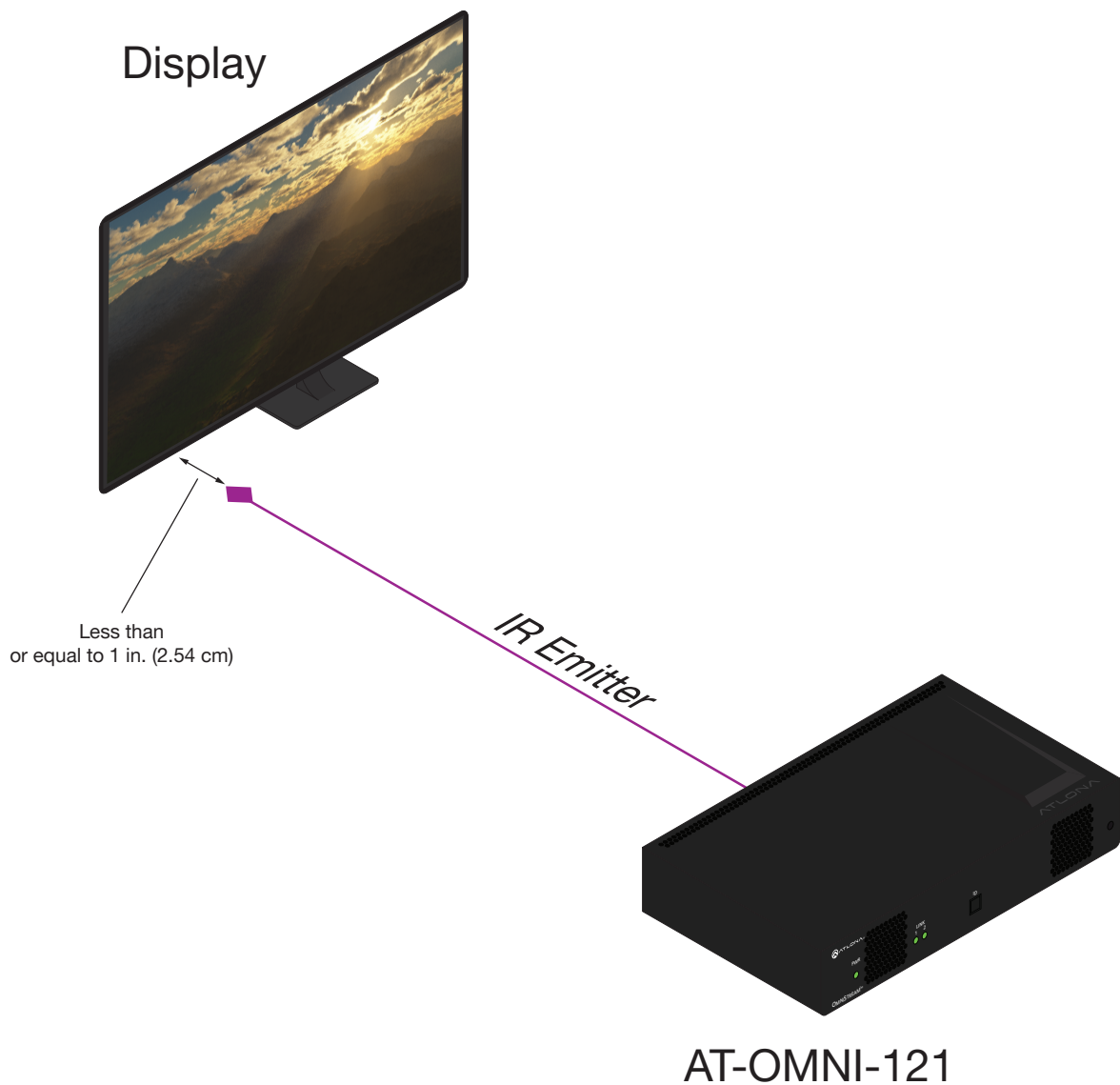
15. Click the **SAVE** button to commit changes.

Serial configuration		Command: Display Off	
Name	serial_use2	Mode	
Port	serial_port2 ▼	ASCII	
Mode	output ▼	HEX	
Input	ip_input5 ▼		
Bidirectional	Interface		<b>SAVE</b> <b>DELE</b>
	Destination IP address	N/A	
	Destination UDP port	5004	
	Enabled	<input type="checkbox"/>	
	<b>SAVE</b>		
		Command: Display On	
		Mode	
		ASCII	
		HEX	

### Testing IR Functionality

1. Point IR remote to at the IR Receiver, as shown in the diagram below.
2. The IR remote will now sent IR data to the decoder where it will be relayed to the display device.

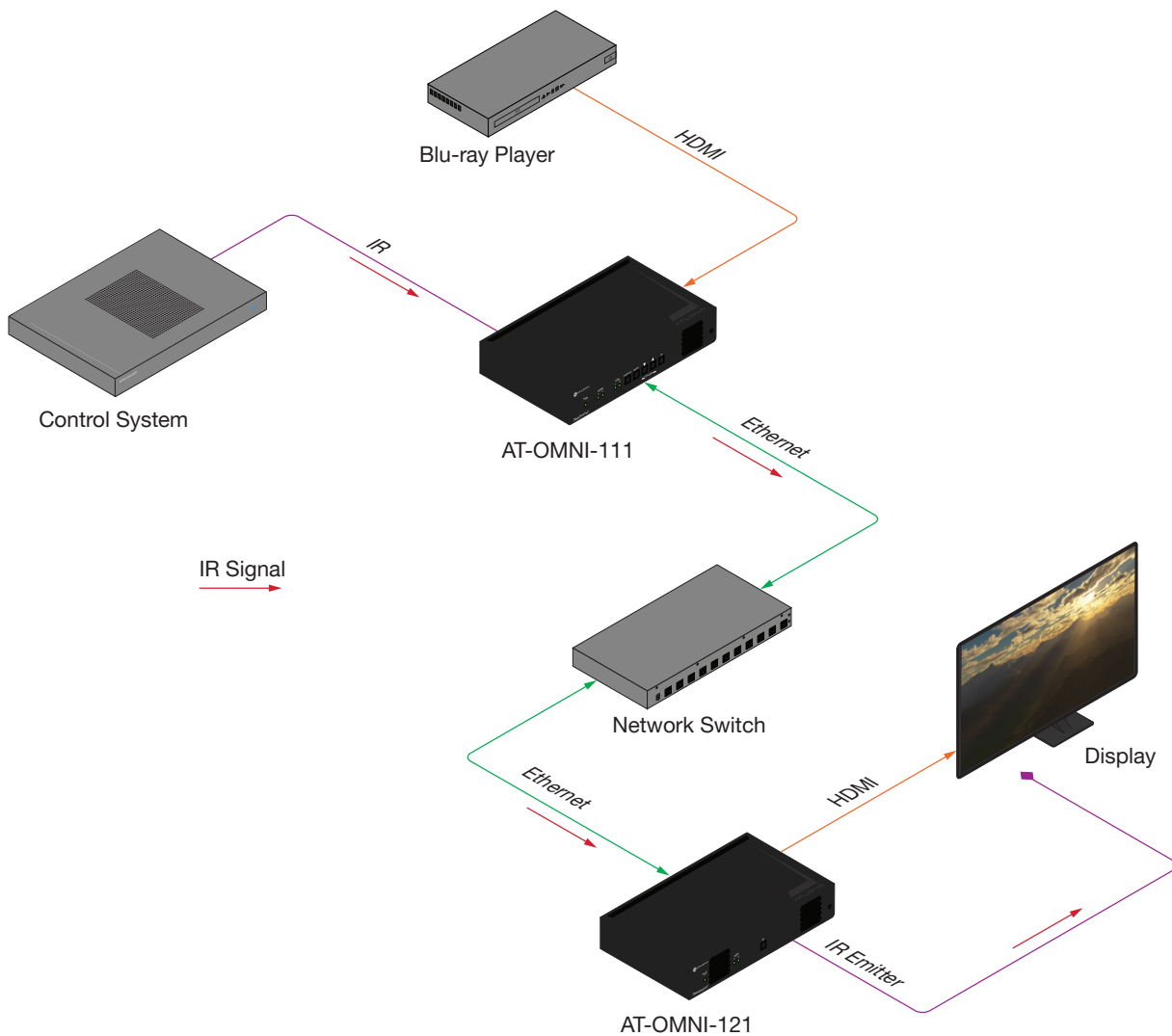
 **IMPORTANT:** The IR lens of the emitter must be within 1 inch (2.54 centimeters) of the IR window on the display device. If this distance is exceeded, then IR functionality may fail.





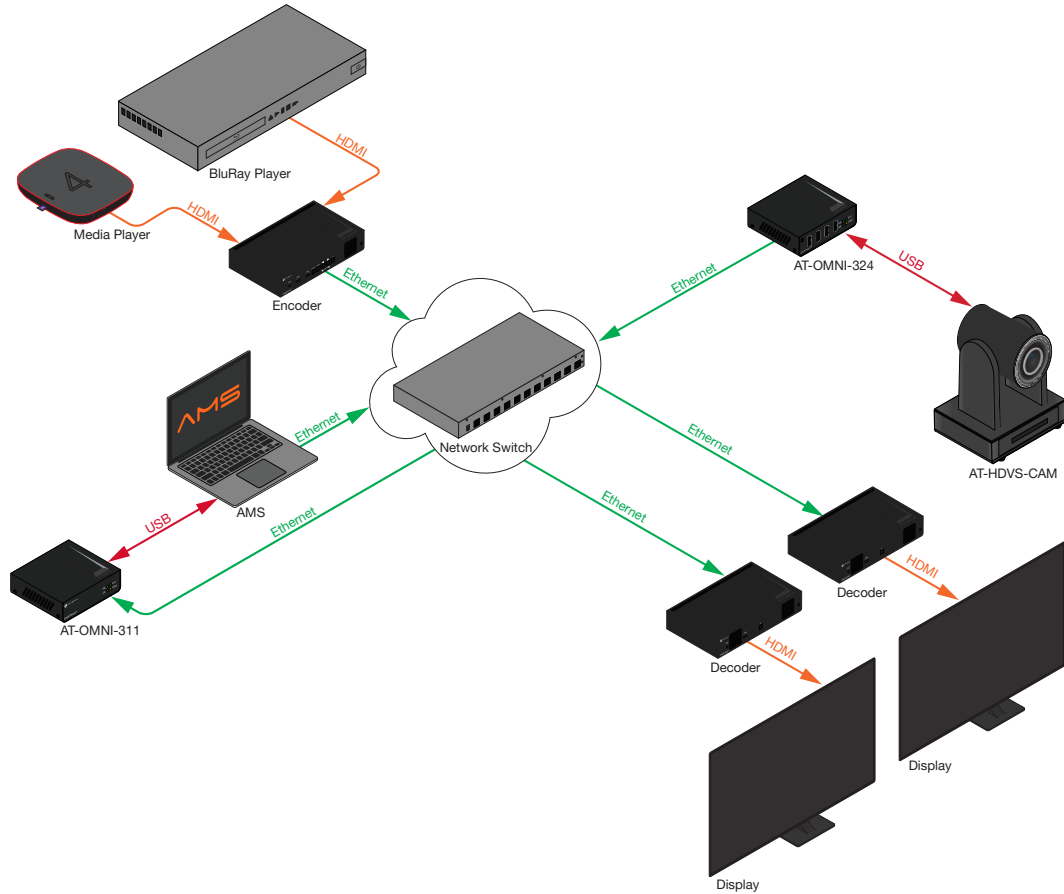
## Controlling the Display using a Control System

The following steps are similar to [Controlling the Display using the Display's IR Remote](#) (page 38), except that the control system wiring should be used, instead of an IR receiver, as shown below.

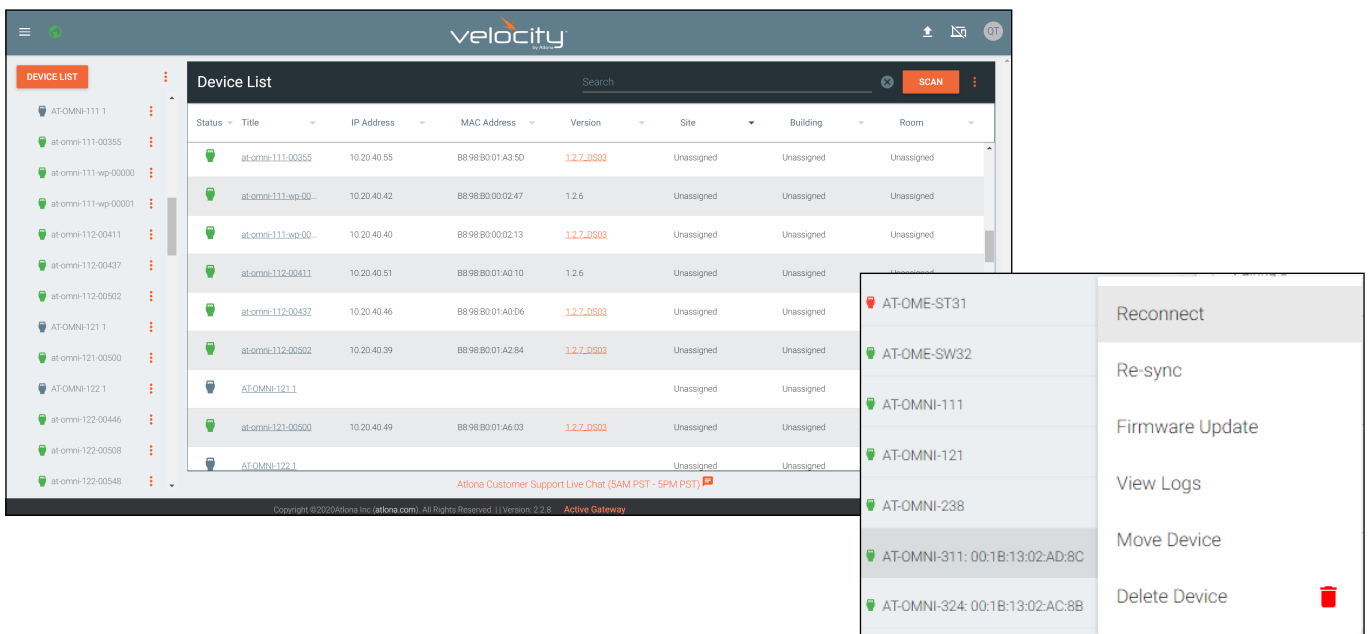


# USB to IP Adapter

OmniStream AT-OMNI-311 and AT-OMNI-324 provide a way to connect USB devices (such as cameras, MICs, etc) over IP.



1. Find the AT-OMNI-311 and AT-OMNI-324 in the left navigation, left click the ;, and select reconnect from the drop down menu.

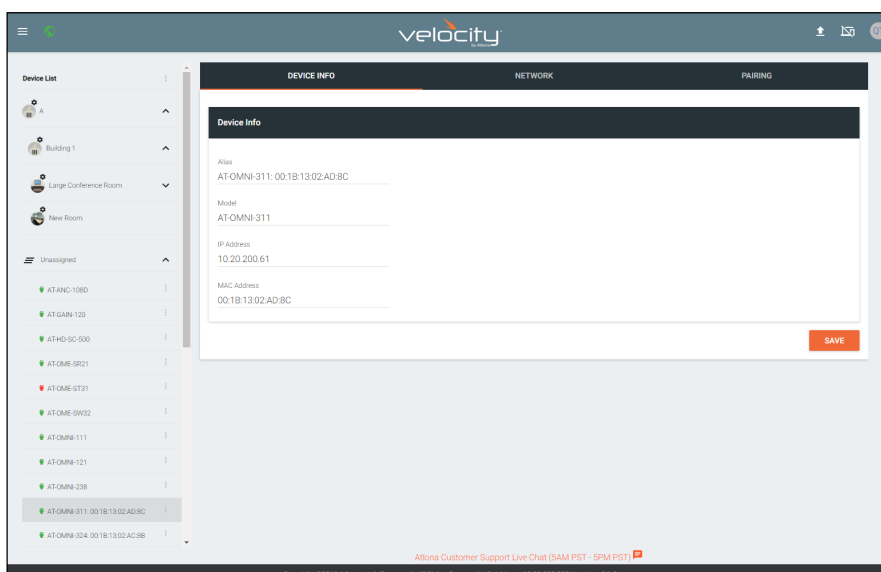


The screenshot shows the Velocity by Atlona web interface. On the left is a 'DEVICE LIST' sidebar with a search bar and a 'SCAN' button. The main area displays a 'Device List' table with columns for Status, Title, IP Address, MAC Address, Version, Site, Building, and Room. A context menu is open over the AT-OMNI-311 device, showing options: Reconnect, Re-sync, Firmware Update, View Logs, Move Device, and Delete Device.

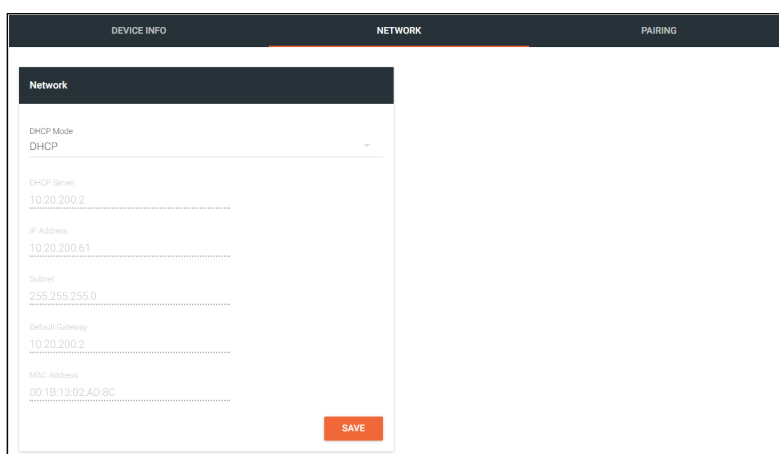
Status	Title	IP Address	MAC Address	Version	Site	Building	Room
AT-OMNI-111.1							
at-omni-111-00355	at-omni-111-00355	10.20.40.55	B8:98:B0:01:A3:5D	1.2.7_0503	Unassigned	Unassigned	Unassigned
at-omni-111-wp-00000	at-omni-111-wp-00000	10.20.40.42	B8:98:B0:00:02:47	1.2.6	Unassigned	Unassigned	Unassigned
at-omni-111-wp-00001	at-omni-111-wp-00001	10.20.40.40	B8:98:B0:00:02:13	1.2.7_0503	Unassigned	Unassigned	Unassigned
at-omni-112-00411	at-omni-112-00411	10.20.40.51	B8:98:B0:01:A0:10	1.2.6	Unassigned	Unassigned	Unassigned
at-omni-112-00437	at-omni-112-00437	10.20.40.46	B8:98:B0:01:A0:D6	1.2.7_0503	Unassigned	Unassigned	Unassigned
at-omni-112-00502	at-omni-112-00502	10.20.40.39	B8:98:B0:01:A2:84	1.2.7_0503	Unassigned	Unassigned	Unassigned
AT-OMNI-121.1	AT-OMNI-121.1				Unassigned	Unassigned	Unassigned
at-omni-121-00500	at-omni-121-00500	10.20.40.49	B8:98:B0:01:A6:03	1.2.7_0503	Unassigned	Unassigned	Unassigned
AT-OMNI-122.1	AT-OMNI-122.1				Unassigned	Unassigned	Unassigned
at-omni-122-00446	at-omni-122-00446				Unassigned	Unassigned	Unassigned
at-omni-122-00508	at-omni-122-00508				Unassigned	Unassigned	Unassigned
at-omni-122-00548	at-omni-122-00548				Unassigned	Unassigned	Unassigned

**NOTE:** Reconnecting the unit before adjusting it will ensure the units will be available in the pairing drop down menu.

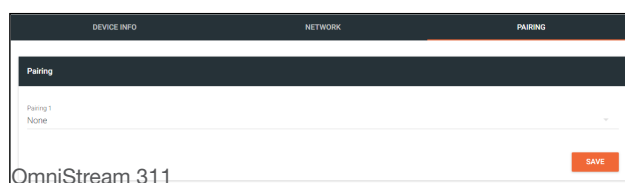
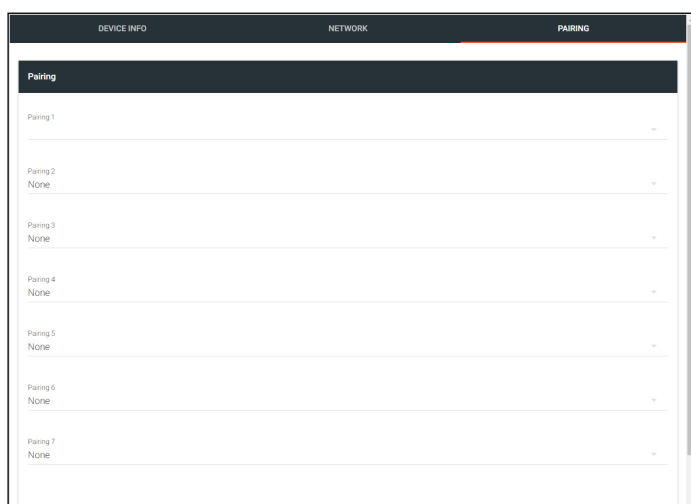
- Select either AT-OMNI-311 or AT-OMNI-324 from the device list. Pairing can be done from either unit, so the following step will show settings updating through OmniStream 311.



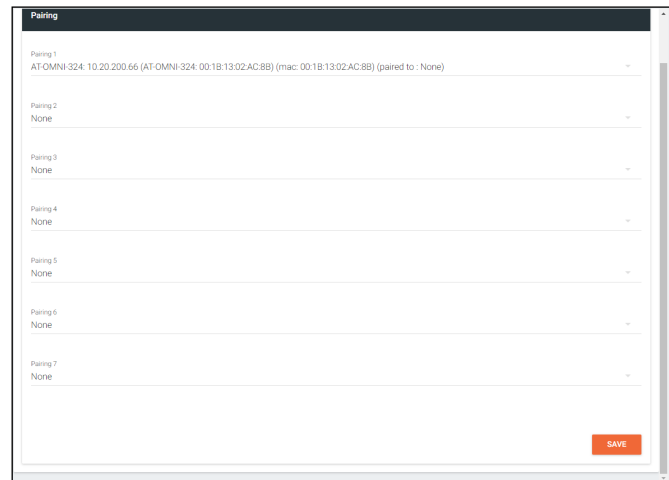
- \*Optional\** The units will be set to DHCP by default. Select Network to adjust the network setting to static mode.



- \*Optional\** Select Static from the DHCP Mode drop down and fill in the IP Address, Subnet, and Default Gateway. **e.g.** 192.168.1.54, 255.255.255.0, and 192.168.1.1
- Select Pairing from the top navigation. These following steps will be the same on either the AT-OMNI-311 or AT-OMNI-324.



- Select the unit to pair to from the drop down menu. The OmniStream 311 can pair with up to 7 USB devices, the OmniStream 324 can pair with only 1 host. It does not matter which drop down is used on the AT-OMNI-311 as it will assign it to any port.
- Press the **SAVE** button once the device has been selected.



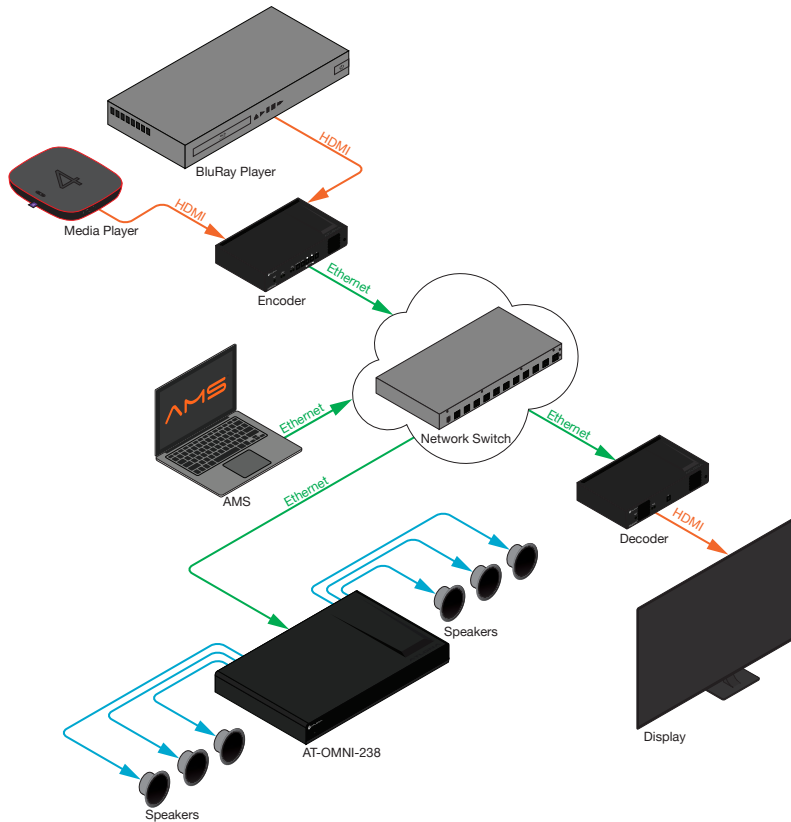
- The devices are now paired. Repeat steps 5 to 7 for all the OmniStream 311s and OmniStream 324s.

# IP to Analog Audio Bridge

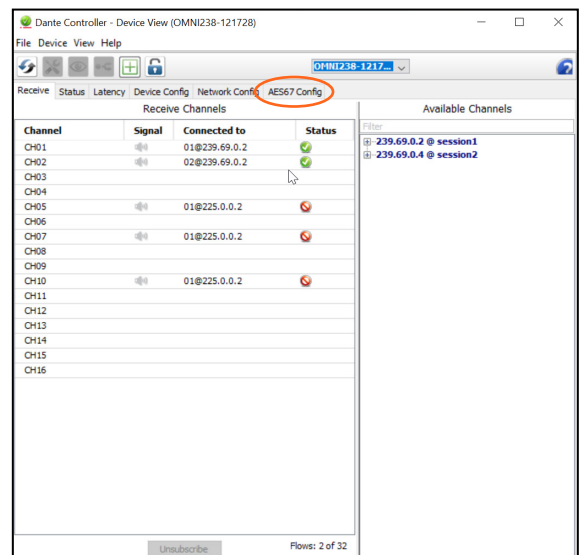
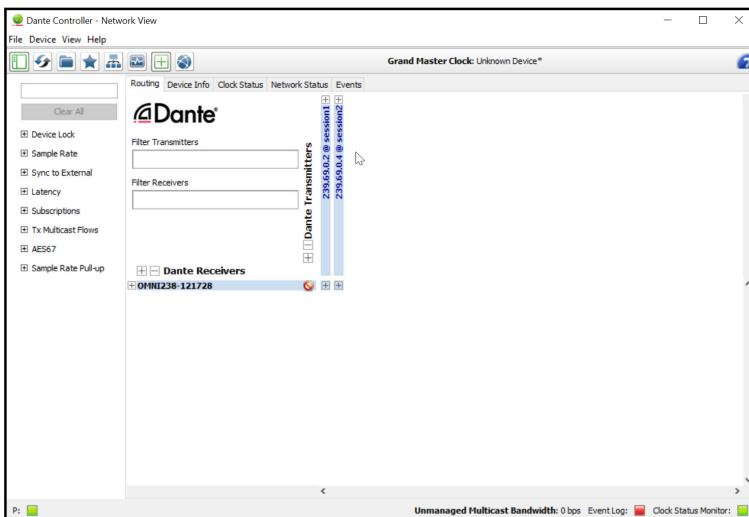
OmniStream 238 can be set up and routed using the Dante Controller. To download the software, go to <http://www.audinate.com>. The software will be found under **products > software > Dante Controller**. The download button is found on the right side of the page. Follow the instructions for downloading.

Once downloaded and installed, the AT-OMNI-238 will be automatically detected as long as the PC running Dante Controller and OmniStream 238 are on the same network.

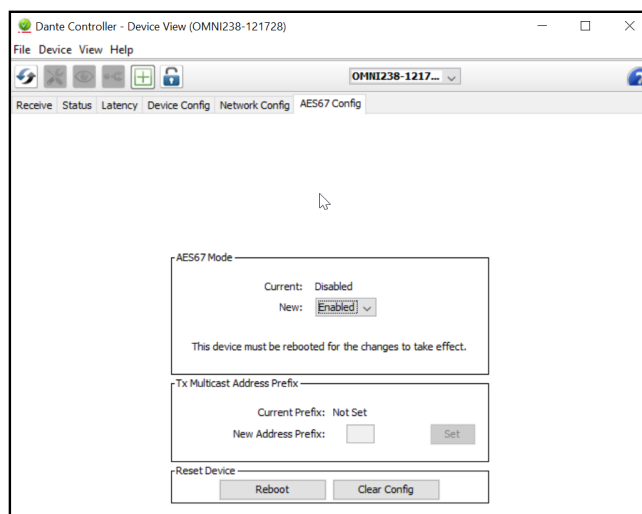
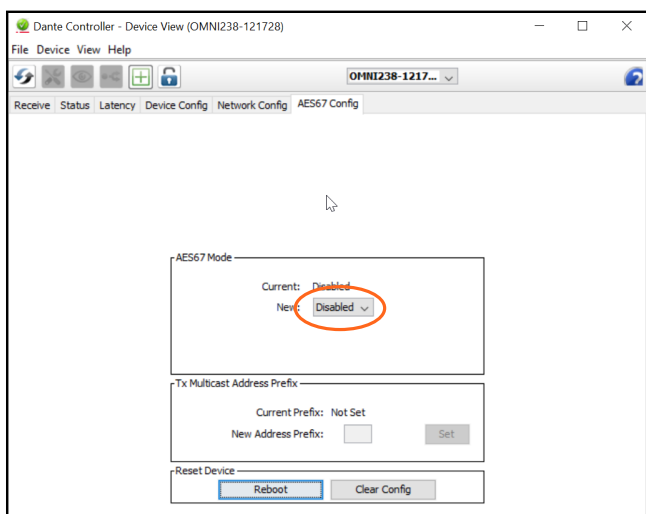
**NOTE:** By default the AT-OMNI-238 will have AES67 disabled and will need it enabled to route the AES67 audio from the OmniStream Encoders.



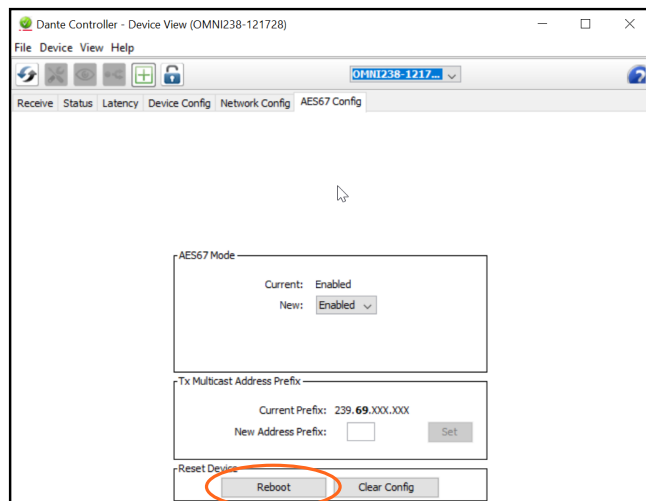
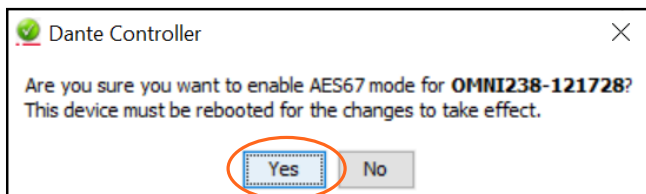
1. Open the Dante Controller application.
2. Double click the OMNI238 under the Dante Receivers. A new window will open.



3. Select AES67 Config from the middle navigation.

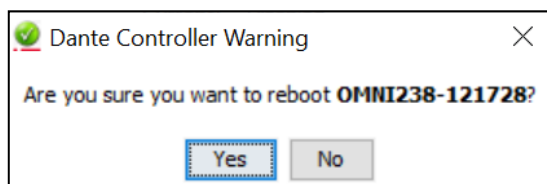


4. Select the **New:** drop down field and select Enabled. A pop up will appear.



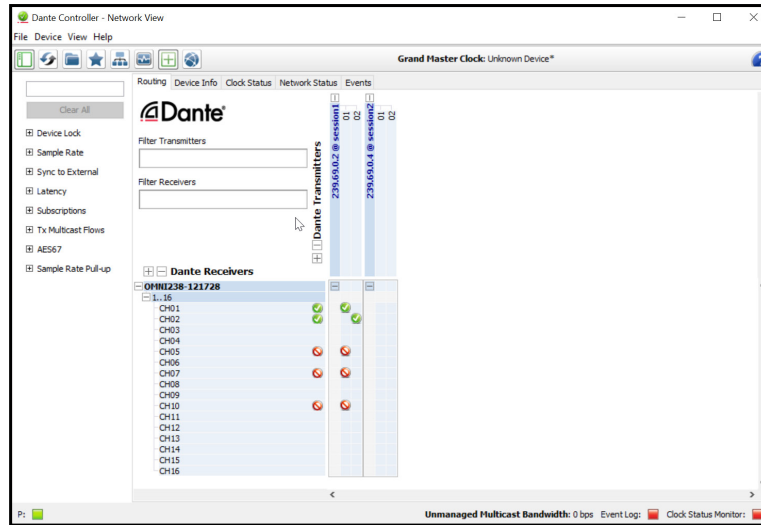
5. Select the **Yes** button to confirm the switch to AES67 enabled.

6. Press the **Reboot** button to restart the AT-OMNI-238 and finish enabling AES67. A new pop up will appear.



7. Select the **Yes** button to confirm the reboot.

The software will return to the home screen when the reboot is finished. AES67 sources will appear as source options for the AT-OMNI-238 in the routing menu once the reboot is finished.



8. Open the streams with the + buttons next to the OmniStream 238 and the multicast addresses of the OmniStream audio streams.
9. Select the cross section squares to route the streams. The streams will only appear as green checks when audio is passing.

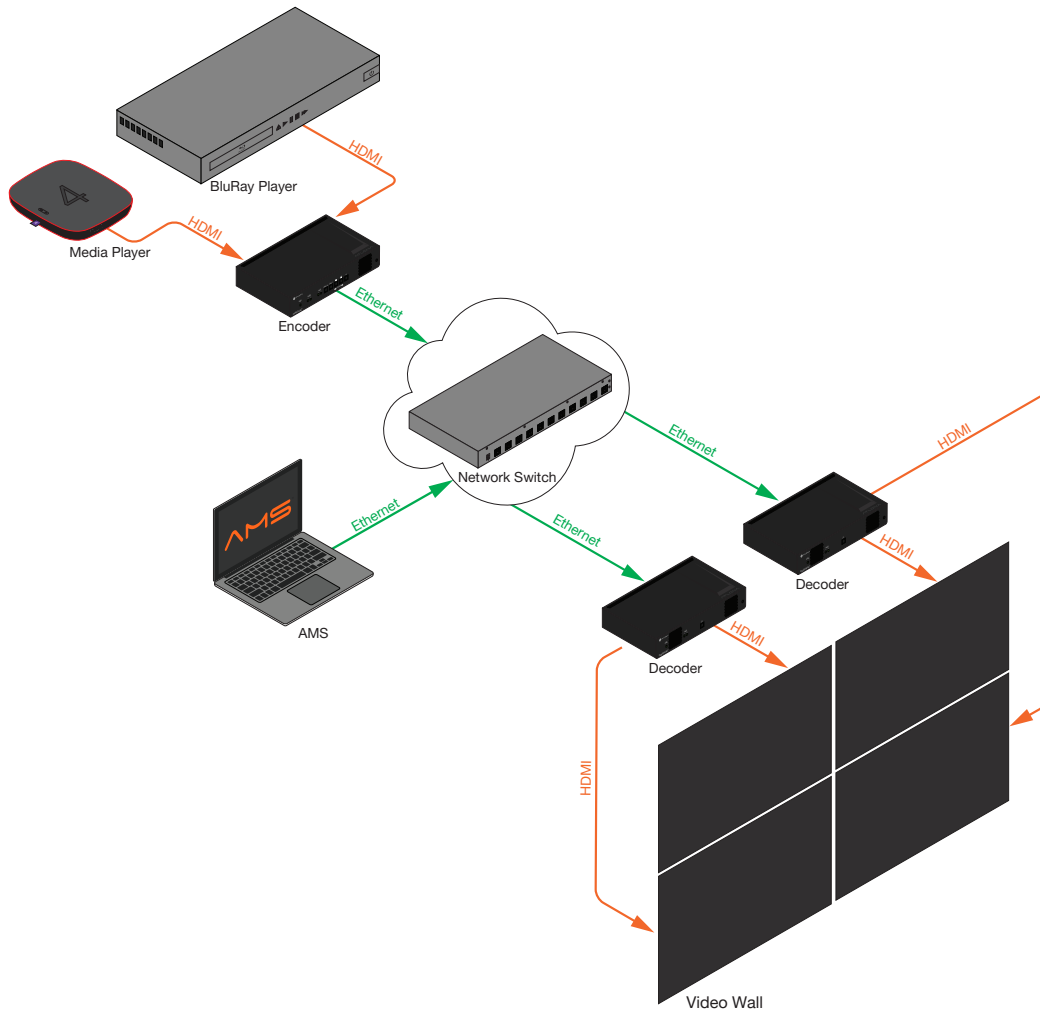


**NOTE:** Audio paths will only show green if there is an active audio signal passing. If there is no active audio passing the connection will show a red icon.

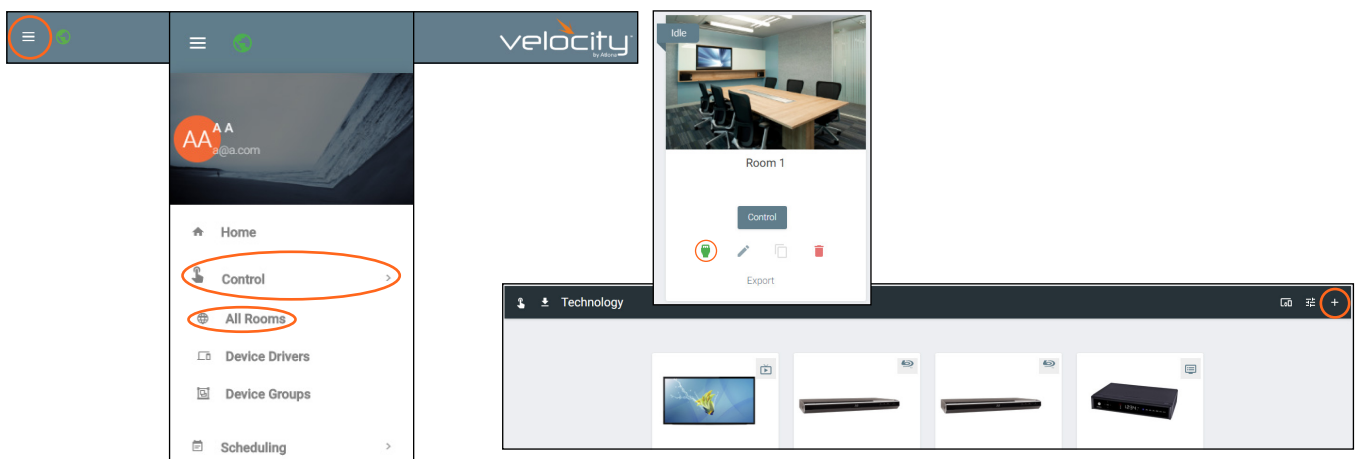
Audio routing should be complete and audio passing.

# Video Walls

After the basic configuration of the devices is finished, the optional video wall can be set up using the room view. The following steps will provide the simplest way to set up a video wall.

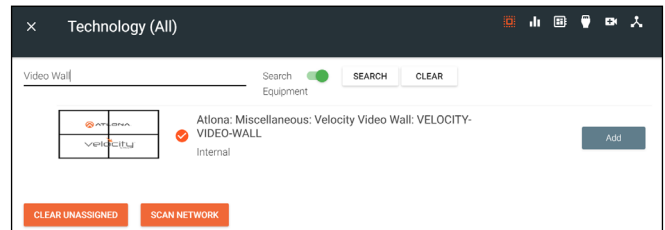
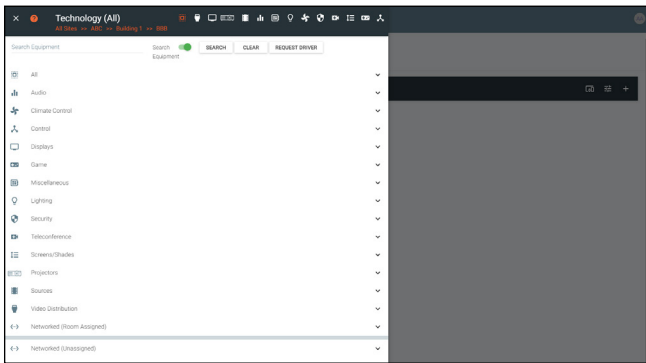


1. Select the ≡ button from the top left corner and select **Control**.
2. More options will appear. Select **All Rooms**. A new screen will open.
3. Select the Edit Room Technology button on the room tile. The Modify Technology screen will open.

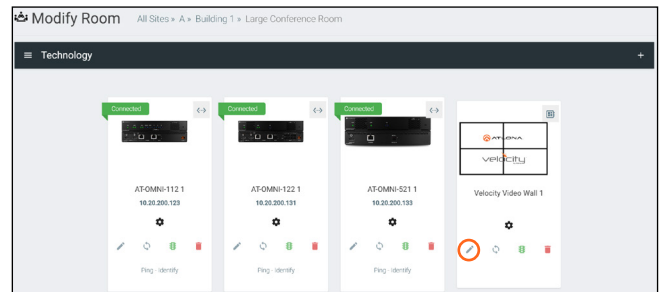
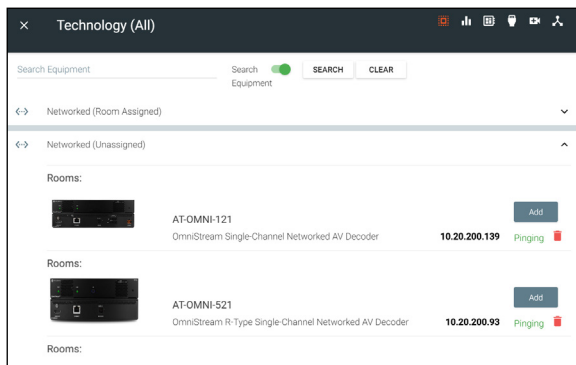




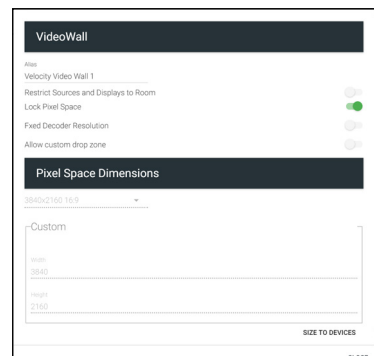
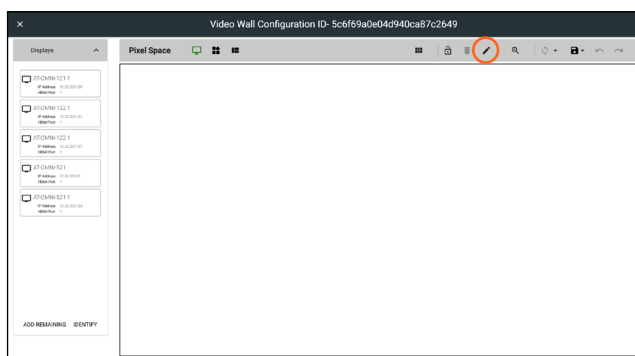
- Press the small + in the top right corner of the Technology header. A new menu will slide open on the left side of the screen.
- Type Video Wall into the search bar and press enter.
- Select the **Add** button next to the Velocity-Video-Wall when it appears.



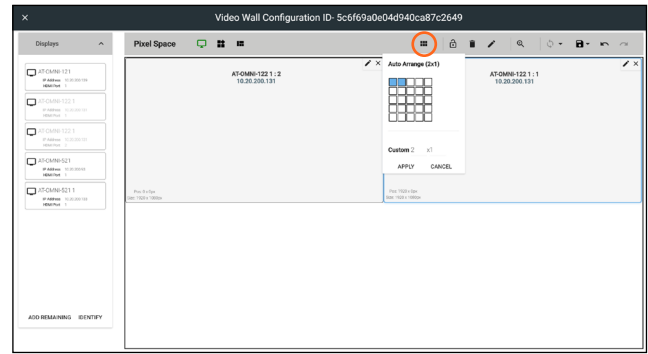
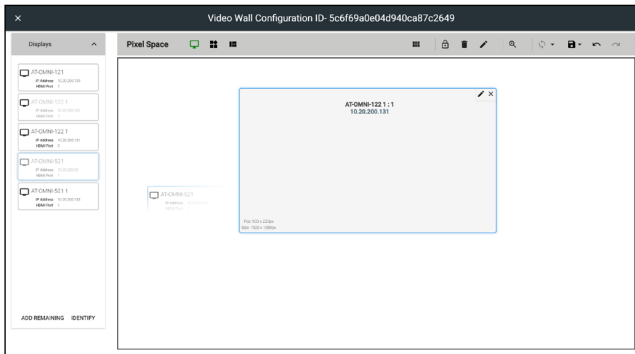
- Press the **Clear** button located next to the search.
- Select the Networked (Unassigned) label, this will expand the field.
- Add all the OmniStream devices associated with the Video Wall.
- Click outside of the menu, or select the **X** at the top to return to the room.
- Select the **Edit** button (circled below) on the Video Wall. The Video Wall configurator screen will open.



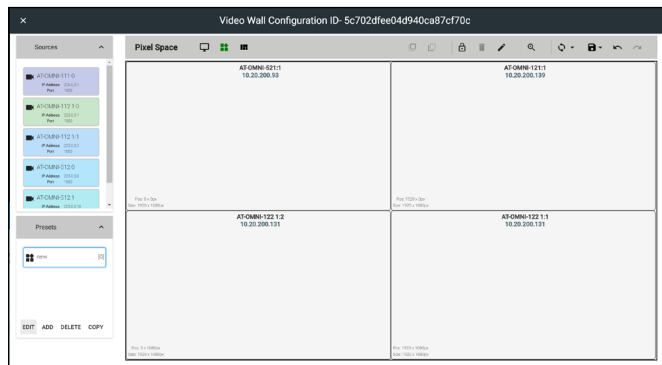
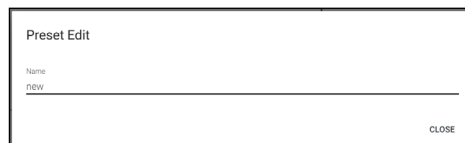
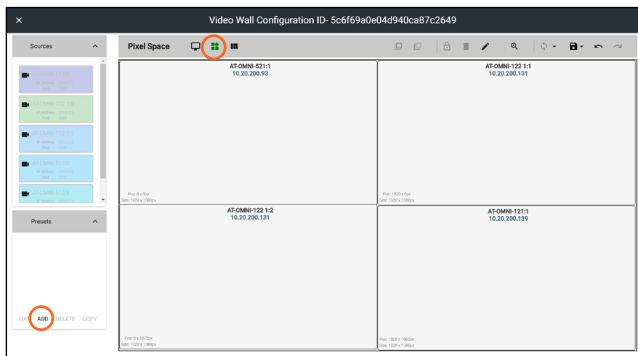
- Select the Edit button. A new pop up window will appear.
  - Alias** - Provide an Alias for the Video Wall.
  - Lock Pixel Space** - This locks and unlocks the resolution of the video wall. By default this is enabled. Disable to select a custom size and resolution in the Pixel Space Dimensions area.
  - Allow custom drop zones** slider - Select this to allow the creation of custom drop zones.
  - Pixel Space Dimensions** - When unlocked, the resolution of the video wall can be selected here.



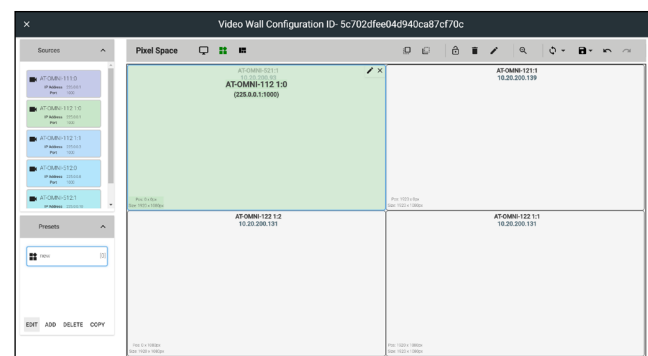
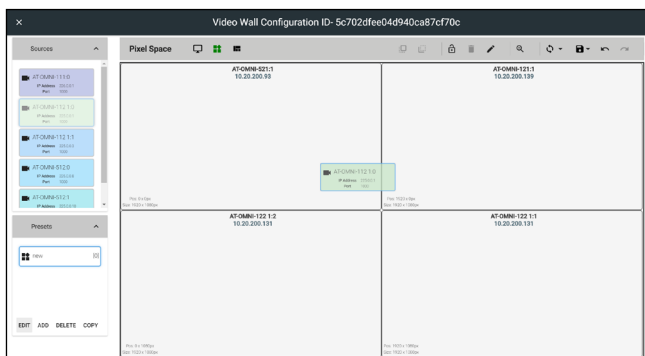
17. Double click or drag and drop the wanted decoders from the Displays area. Only drag and drop the decoders that will be used for the video wall.
18. Auto arrange the displays by dragging a mouse over the grid to the correct display layout and left clicking.



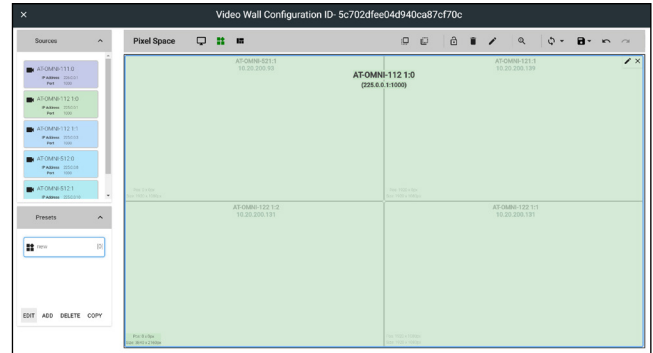
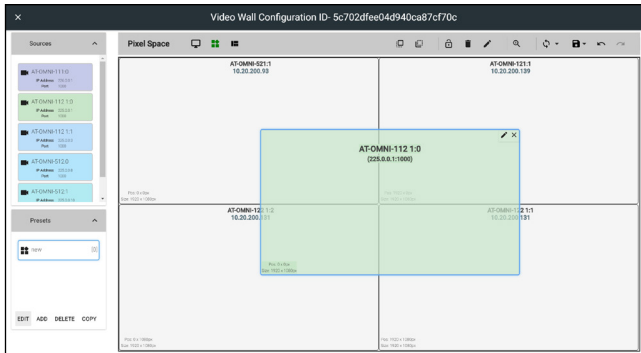
19. Select the **Preset** button (circled below) to have sources and presets become available for selection and adding.
20. The sources will not be selectable until a preset has been added, press the **ADD** button (circled below) in the Presets field. A pop up will appear.
21. Name the preset and press the enter key to close or select the close button.
22. Add as many presets as needed.



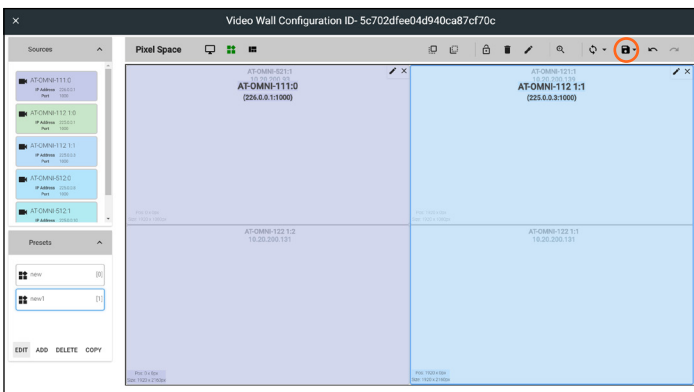
23. Select the source and drag and drop it into the decoders. The source will appear over one of the displays as a different colored square.



24. Select the source square and arrange it over the decoders it should display on. Placing it centered over intersecting lines will have it fill up all the connected decoders.



25. Repeat for each configuration needed.



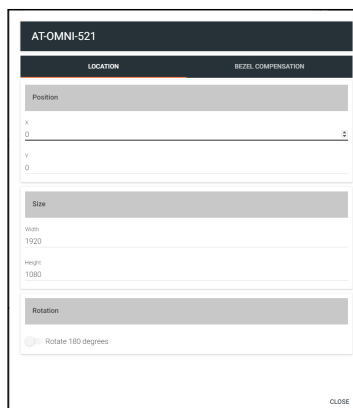
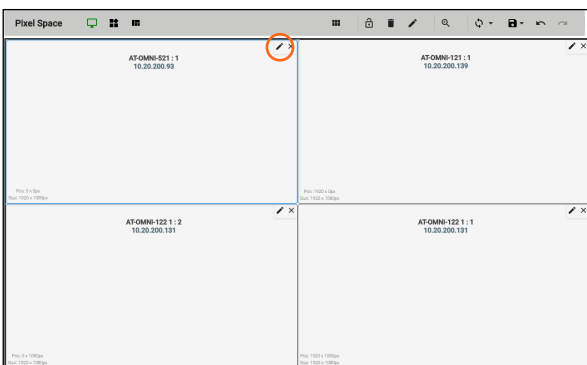
- NOTE:** The preset being currently set is highlighted in blue on the left.
- NOTE:** Multiple sources can be used in a preset, each will show up in different colors.

If the video wall picture is satisfactory, continue with step 26. If picture adjustment is needed to compensate for the display's bezel, continue to step 27.

26. Select the **save** button (circled above) and exit out of the configuration screen once complete.

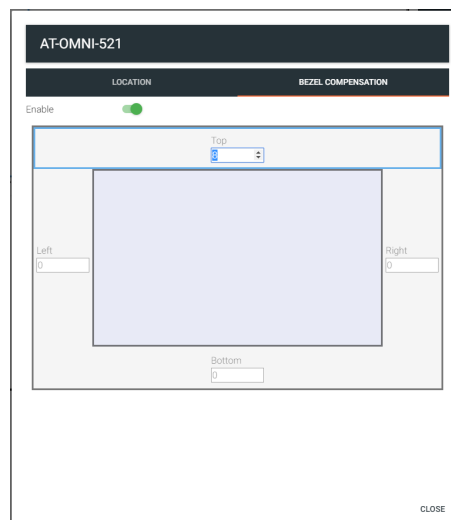
27. Select the **edit** button (circled below) on the top right of the display field. A pop up will appear.

28. Select the Bezel Compensation tab.



29. Select the Enable slider to allow for bezel compensation. The bezel fields will unlock.

30. Type or use the arrows to adjust the bezel pixel size in each area that requires compensation. e.g. If the display is in the top left of the video wall, the right and bottom bezel should be compensated for.



**NOTE:** If the bezel needs to be adjusted for in a format other than pixel, return to the device view within the device list from configuration and open the HDMI OUTPUT tab. Scroll to the under the Video Wall slider and select the unit type for adjustment (Pixels, Millimeters, or Inches). Select the **SHOW ADVANCED** button, then select **Bezel Compensation** from the Edge Compensation drop down and then enter the correct amount, before pressing the save button.

