Matrox® Avio™ N2150

Installation and User Guide

Part No.: 20366-301-0100

Last Updated: July 11, 2025
(Go to our *website* for the latest version)

Trademarks

Trademarks • Marques déposées • Warenzeichen • Marchi registrati • Marcas registradas

Matrox Graphics Inc.	Matrox®
Microsoft Corporation	Microsoft® Windows®
Google LLC	Chrome™
Apple	Bonjour®

All other nationally and internationally recognized trademarks and tradenames are hereby acknowledged.

See the Matrox Software License Agreement: *https://video.matrox.com/software-license-agreement*

See the product's hardware warranty: *https://video.matrox.com/en/support/warranty/*

Disclaimer: Matrox Graphics Inc. reserves the right to make changes in specifications at any time and without notice. The information provided by this document is believed to be accurate and reliable. However, no responsibility is assumed by Matrox Graphics Inc. for its use; nor for any infringements of patents or other rights of third parties resulting from its use. No license is granted under any patents or patent rights of Matrox Graphics Inc. Unauthorized recording or use of broadcast television programming, video tape, or other copyrighted material may violate copyright laws. Matrox Graphics Inc. assumes no responsibility for the illegal duplication, use, or other acts that infringe on the rights of copyright owners.

Matrox Graphics Inc.
1055 St. Regis Blvd., Dorval, Quebec, Canada H9P 2T4
Tel: (514) 685-2630 Fax: (514) 685-2853 World Wide Web: https://video.matrox.com

Table of contents

Chapter 3: Using Avio 2

Chapter 4: Matrox Avio 2 Receiver settings

Chapter 5: Matrox Avio 2 Transmitter settings

Chapter 6: Hardware specifications

Chapter 7: Customer support

CHAPTER 1

Introduction

This chapter includes the following topics:

About Matrox Avio 2

The award-winning Matrox Avio N2150 IP KVM extender ensures secure, real-time performance for mission-critical applications that need remote access to computing equipment, delivering unparalleled image quality and support for up to 4K resolution. By leveraging open standards like IPMX, SMPTE 2110, and NMOS, Avio 2 future-proofs your KVM System over IP installation with a scalable, flexible, and easy-to-use solution. Designed for seamless integration with evolving networked infrastructures, Avio 2 is ideal for control rooms, medical applications, broadcast studios, media production, and live events.

For more information on Matrox Avio 2, see our *website*.

About the Matrox Avio 2 user documentation

The Matrox Avio 2 documentation includes the following resources:

- Matrox Avio 2 Device Setup Sheet

Each Avio 2 device ships with a printed quick start sheet. It covers hardware connections and the basic setup steps to get you started. A PDF version is also available on the Matrox Video *website*.

- Matrox Avio N2150 Installation and User Guide

This is the main user guide for configuring and operating the Avio 2 device. You can download it from the Matrox Video *website*, along with the latest firmware. Always refer to the website for the most recent version of the guide.

Matrox safety information

⚠ To ensure safe and reliable operation of your Matrox product, to avoid personal injury, and to prevent damage to your computer or Matrox hardware, read the following guidelines.

Installation and operation

- Read and retain all instructions. Only use your Matrox product according to the instructions, operating ranges, and guidelines provided in the Matrox user guide and other related Matrox documentation. Failure to follow these instructions could result in damage to your product or injury to the user or installer.
- Don’t expose your Matrox product to rain, water, condensation, or moisture.
- Caution: Hot Surface, Do Not Touch
  Your Matrox product can become hot while operating. Ensure that your computer cover is secured in place before turning it on.
  Always turn off your computer, unplug it, and then wait for it to cool before removing the cover of your computer to touch any of its internal parts or to install your Matrox card. Allow hot surfaces to cool before touching your Matrox unit.
- **Attention: Surface chaude, ne pas toucher**
  Votre produit Matrox peut devenir chaud durant son fonctionnement. Assurez-vous de bien fermer le couvercle de votre ordinateur avant de l’allumer.
  Éteignez votre ordinateur, débranchez-le et attendez qu'il refroidisse avant d'ouvrir son couvercle pour accéder à ses parties internes ou pour installer votre carte Matrox. Laissez les surfaces chaudes refroidir avant de toucher votre appareil Matrox.
- Static electricity can severely damage electronic parts. Before touching any electronic parts, drain static electricity from your body (for example, by touching the metal frame of your computer).
- When handling a card, carefully hold it by its edges and avoid touching its circuitry.
- Don’t stack devices or place devices so close together that they’re subject to recirculated or preheated air.
- Don’t operate your system or Matrox product near a heat source or restrict airflow to your system, and make sure the ambient temperature doesn’t exceed the maximum recommended temperatures. Don’t block ventilation holes on your unit or system.

If a power supply (internal or external) was included with your product

- Don’t place the external power supply directly on top of the device.
- Only use power supplies originally supplied with the product or use a replacement that’s approved by Matrox. Don’t use the power supply if it appears to be defective or has a damaged chassis.

- Any AC-powered product must be connected to a grounded outlet installed by a licensed electrician. Don’t defeat the safety purpose of the polarized or grounding-type plug. A polarized plug has two blades with one wider than the other. A grounding-type plug has two blades and a third grounding prong. The wide blade or the third prong are provided for your safety. If the provided plug doesn’t fit into your outlet, consult a licensed electrician to replace the obsolete outlet.
- Make sure that nothing rests on the power cables and that the cables aren’t located where they can be stepped on, pinched, or tripped over.
- Don’t use damaged power cables.
- Unplug your system or device during lightning storms or if unused for long periods of time.

If your product includes laser-based technology

- The device contains a Class 1 laser product for use only under the recommended operating conditions and guidelines. For more information, see your Matrox user guide.
- Invisible laser radiation may be emitted from disconnected fibers or connectors. Don’t stare into beams or view directly with optical instruments.
- Only use optical transceivers originally supplied with the product or use a replacement that’s approved by Matrox.
- For more information on laser support and compliance, see your Matrox user guide.

If your product includes a battery

- The battery is non replaceable.
- To dispose your product, see https;//video.matrox.com/en/environment/product-waste-management.

Repair

- Don’t attempt to open or repair a power supply unit (if one was supplied).
- Don’t attempt to open or repair your Matrox product.
- If there’s a fault with your Matrox product, review your Matrox warranty for more information.

Supported web browsers

You configure and control the Matrox Avio 2 device through a web-based user interface.

Google Chrome is officially supported by Avio 2.

Other browsers such as Microsoft Edge may work, but have not been tested or validated by Matrox Video.

About the Matrox Unified Utility

The Matrox Unified Utility is a free application that simplifies the deployment and management of Matrox Video devices on IP networks. The utility reduces setup time and improves efficiency by streamlining key deployment tasks. For more information, refer to the Matrox Unified Utility User Guide on the Matrox Video *website*.

CHAPTER 2

Getting started with Matrox Avio 2

This chapter includes the following topics:

- *Device connections and button functions*
- *Discovering your Avio 2 device on the network*
- *Before you begin*
- *Initial setup overview*
- *Device properties*
- *Switching between the Avio 2 operation modes*
- *Firmware update*
- *Preferences*
- *Troubleshooting*

Device connections and button functions

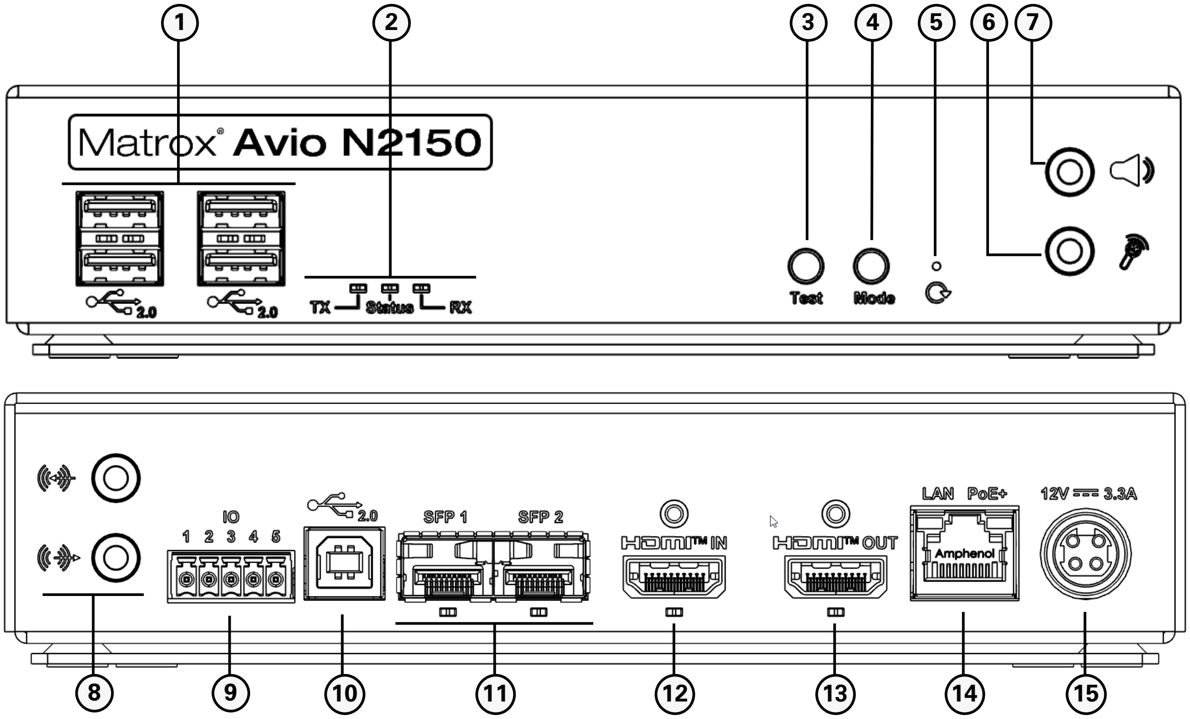
The information in this section is also available on the printed Matrox Avio 2 Device Setup Sheet included with your Matrox Avio 2 box.

The setup sheet describes the device’s hardware connections and button functions. You can also download the latest versions from the Matrox Video *website*, along with the most recent firmware.

Matrox Avio 2 transmitters and receivers

The following components are available on the Matrox Avio 2 front and rear panels.

NOTE The Matrox Avio 2 device images have been intentionally simplified for illustration purposes.



Button/Connector/LED	Description
(1) - USB 2.0 (Type A)	**Tx mode** - Connect a local keyboard and mouse. **Rx mode** - Connect USB 2.0 peripheral devices, such as a keyboard and mouse.
(2) - Status LEDs	Indicates general device status and shows if the Avio 2 is in Transmitter (Tx) or Receiver (Rx) mode.

Button/Connector/LED	Description
(3) - Test	**Tx mode** - Press for 5 seconds to activate Test pattern. Press again for 2 seconds to return. **Rx mode** - Not used.
(4) - Mode	**Mode switch** - Press with **Reset** for 4 seconds to switch between Tx / Rx.
(5) - Reset	**Reset** - Press for 3 seconds to reboot, or 10 seconds to reset to factory defaults. **Mode switch** - Press with **Mode** for 4 seconds to switch between Tx / Rx.
(6) - Mic-in	**Tx mode** - To be supported in a future release. **Rx mode** - To be supported in a future release.
(7) - Headphones	**Tx mode** - To be supported in a future release. **Rx mode** - Connect headphones or other audio devices.
(8) - Line IN / Line OUT	**Tx mode** - Connect analog audio source. **Rx mode** - Line OUT is used.
(9) - IO	To be supported in a future release.
(10) - USB 2.0 (Type B)	**Tx mode** - USB connection to host system. **Rx mode** - Not used.
(11) - SFP 1 / SFP 2	Connect one or both SFPs to your media network for streaming. Ensure that the SFPs are connected to Avio 2 before you power on the device. The “hot plugging” of SFPs is not supported. **NOTE**: Resolutions up to 4Kp30 can be streamed using one SFP. To stream 4Kp60, you need two SFPs to be connected.
(12) - HDMI IN	**Tx mode** - Connect to video output of source system. **Rx mode** - Not used.
(13) - HDMI OUT	**Tx mode** - Connect an HDMI monitor to view the HDMI IN video passthrough. **Rx mode** - Connect an HDMI monitor.
(14) - LAN / PoE+	Connect to control network (optional) and provide Power over Ethernet (PoE+).
(15) - Power	If PoE+ is not being used, connect a 12V d.c. power supply (sold separately).

Discovering your Avio 2 device on the network

When you power on your Matrox Avio 2, it starts in Receiver (Rx) mode and gets an IP address from your DHCP server. If a monitor is connected during startup, the IP address appears on the On-Screen Display (OSD).

Before you begin

The Avio 2 user interface is similar whether accessed from a Web browser or through the On-Screen Display (OSD).

Matrox Avio 2 terminology

In the Avio 2 user interface and documentation, the abbreviation “Tx” may be used to indicate a transmitter, depending on the context. Also, “Rx” may be used to denote a receiver.

Initial setup overview

This section describes the essential steps that you need to perform to bring your Avio 2 device to a functional state.

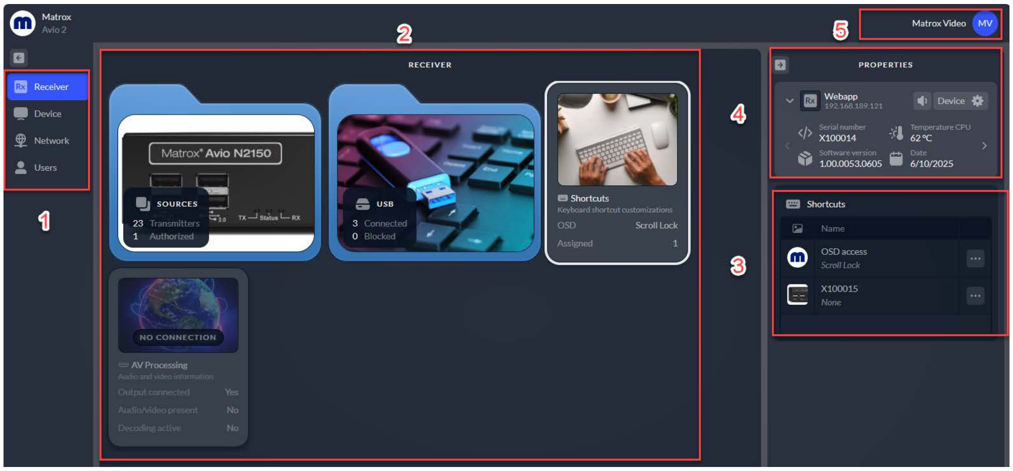
Access the user interface

The Avio 2 device’s user interface can be accessed by two means:

- Rx - Through the On-Screen Display (OSD) - The OSD displays on a monitor that is connected to the device. (Make sure a monitor is connected to the receiver to be able to access the OSD.) You can also access the OSD by using the shortcut keys. The default shortcut key to access the OSD is **Scroll lock**. You need to be logged into the OSD to be able to access the OSD using shortcut keys.
- Rx and Tx - Through the web-based user interface via web browser - In a web browser such as Google Chrome, you can type the IP address of the device to access the web user interface.
  - If the web browser is in the same network subnet as the device, you can use the DNS name of the device instead of the IP address. The default DNS name of the device is “**mtxav2-**” followed by the device's serial number in lowercase. For example, a device with its serial number as AB13245 can be accessed by typing https://mtxav2-AB12345.local in the Google Chrome address bar.
  - If the above method is unsuccessful, try disabling the proxy and using the URL.

User interface overview

The web-based user interface has five key areas.



23 Transmitters
1 Authorized

3 Connected
0 Blocked

Shortcuts
Keyboard shortcut customizations
OSD Scroll Lock
Assigned 1

AV Processing
Audio and video information
Output connected Yes
Audio/video present No
Decoding active No

Webapp 192.168.189.121
Serial number X100014
Temperature CPU 62 °C
Software version 1.00.0053.0605
Date 6/10/2025

Shortcuts
Name
OSD access Scroll Lock
X100015 None

- **(1) Navigation menu (left)** - Displays the main menu options on the left of the interface. Let’s you move between the main sections.
- **(2) Tiles (center)** - Displays the sub-options available for the selected option from the left navigation menu.
- **(3) Panel (right)** - Displays details of the selected tile and also lets you set the options.
- **(4) PROPERTIES section (top right)** - A carousel that displays on the top right from where you can see important details about the device such as the current software version, temperature, etc., and also carry out device operations such as updating the firmware and rebooting the device. This section displays perpetually, no matter which menu option you select. You can navigate within the section using the left and right arrows.
- **(5) User details - (top right corner)** - Displays the user logged-in, information about the software version, user preferences, troubleshooting, and also log out from here.

Perform initial configuration (out-of-the-box connection)

Through the user interface, you need to perform some initial configuration steps to bring the Avio 2 device to an operational state. You need to do this once you unbox the device, or after doing a configuration reset of the device. The steps given below are for a basic configuration that enables out-of-the-box quick connection, making use of most default settings.

To do the initial configuration:

Step 1. **Connect your hardware**: Start by making all the hardware connections on your Avio 2 devices - power (PoE or external), network, HDMI cables, analog audio, and USB. See "*Matrox Avio 2 transmitters and receivers*" on page *8* for component descriptions to help you connect.

Step 2. **Create the first administrator account and other users**: When you connect to your device from the web browser, a login screen displays where you need to create the first administrator account. For more information, see "*Admin user*" on page *68*. Next, you need to accept the software license agreement that displays. You can then proceed to create other local or domain, admin or regular users. You could do this by importing a JSON file with users list or create individually. For more information, see "*User accounts*" on page *69*.

Step 3. **Set the operational mode**: You need to set the operational mode for each device as either a Tx or Rx. The device starts up in Rx mode. For more information see "*Switch between the device modes*" on page 21.

Step 4. **Rx - Authorize Tx devices**: Using the Rx user interface, authorize the Tx devices to which the receiver can connect. For more information, see "*Authorize a source (transmitter)*" on page *38*. **NOTE**: All Avio 2 transmitters connected to the same network (same subnet) as the Avio 2 receiver will automatically show up on the Sources list in the receiver user interface. Transmitters outside the subnet will display only when the transmitters and the receiver are configured to communicate with an NMOS registry server.

Step 5. **Rx and Tx - Upload JPEG license**: Avio 2 comes with support for Pro AV. You need to upload your JPEG XS license if you want to use the JPEG XS codec. For more information, see "*Licenses*" on page *56*.

Step 6. **Tx - Reboot device**: To set up as a Tx, after changing the operational mode to Tx, reboot the device. For more information see "*Reboot device*" on page 21.

Step 7. **Tx - Enable connecting to multiple receivers:** This step is not required for a one-to-one Tx to Rx connection. For a one-to-many configuration (one Tx to multiple receivers), from the Tx web user interface > Access control > Shared connection, you need to change from **Disabled** to **Audio, video, and USB** or the **Audio, video** option to enable multiple receivers to connect to the Tx.

Step 8. **Start using Avio 2**: Since Avio 2 comes with the required licenses, certificates, encryption, codec, network and USB support, there is nothing further you need to do for the devices to start connecting and streaming. Users on the receiver will now be able to perform their main tasks of connecting to a transmitter, disconnecting from a transmitter, and switching to another transmitter using the web or OSD user interface. For more information, see "*Using Avio 2*" on page *28*.

The admin can continue to perform other less essential tasks such as creating folders, grouping transmitters, setting preferences, changing the default rule for USB groups, and more.

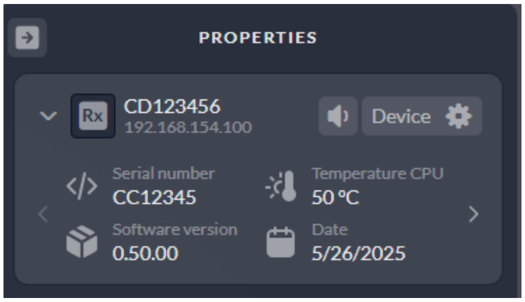
Customize settings

When your connection and streaming requirements are different from the provided defaults, you can customize your settings. Log in as an Admin and make your changes as required. Some of the main ones are provided below.

- **Update firmware (if necessary)**: Check the Matrox Video website to see if a more recent firmware version is available. It is recommended to always use the latest version. For more information, see "*Firmware update*" on page *23*.
- **Change to a different security certificate**: See "*Receiver settings*" on page *33*.
- **Change encryption settings**: See "*Add an encryption key and ID pair*" on page *49*.
- **Enable PTP time setting**: PTP is disabled by default. Enable PTP if required, to be used when streaming audio and video. For more information, see "*Time*" on page *50*.
- **Tx and Rx - Set the EDID**: Download the EDID for your monitor profiles from the Matrox website and upload them to Avio 2. For more information, see "*EDID*" on page *52*.
- **Specify your NMOS registry**: If you plan on using NMOS, specify the NMOS registry server that will be used by Avio 2. For more information, see "*NMOS*" on page *57*.
- **Change network settings**: Select or enter values according to best practices, within the specifications that the Avio 2 device supports. For more information, see "*Network settings*" on page *62*.
- **Rx - Set shortcut keys**: An admin user can set the shortcuts keys to be used for switching and also for displaying the OSD. For more information, see "*Set the shortcut keys*" on page *41*.
- **Tx - Enable link redundancy**: The first release of Avio 2 supports audio and video redundancy. USB will be supported in a future release. **NOTE**: Link redundancy is not available for uncompressed stream resolutions above 4kp30.
- **Tx - AV processing**: The admin on the transmitter will be able to copy the SDP file URL to the clipboard when NMOS is enabled.

Device properties

The device properties section displays perpetually on the top right of the screen under the **PROPERTIES** section, regardless of which menu option you select from the left navigation menu.



PROPERTIES

Rx CD123456
192.168.154.100

Device

Serial number
CC12345

Temperature CPU
50 °C

Software version
0.50.00

Date
5/26/2025

You can expand or collapse and navigate using the arrow buttons in this section.

Setting	Description
PROPERTIES	
Device name, IP address	The friendly name of the device and its IP address.
Audio icon	Rx - You can adjust the analog audio volume by clicking the audio icon and dragging the bar button to the required volume. You can mute the audio by clicking on the mute (🔇) icon.

Device	Get the device information, rename the device, switch the device mode, update the firmware, reboot the device, or reset the device configuration. • **Device info:** The **DEVICE INFO** screen displays the **Serial number, Package version, Date manufactured, Product SKU, PCB revision, Vendor IDs,** and **Device IDs**. • **Rename device:** The default name for a device is the serial number. You can change the name from here. Enter the **Name** and **Description** for the device in the **RENAME DEVICE** screen. • **Device mode:** An Avio 2 device can be configured as either a transmitter or a receiver. Select **Transmitter** or **Receiver** in the **Device name** field in the **DEVICE MODE** screen. For more information see "*Switch between the device modes*" on page 21. • **Firmware update:** Displays the **UPDATE FIRMWARE** screen. The current firmware version is displayed in the **Current version** field. Select the .pkg file by clicking the **Choose file** button from the **Choose a firmware package** field. For more information see "*Firmware update*" on page 23. • **Reboot:** In the **REBOOT** screen, select **Yes** to reboot the device or **No** to cancel. • **Reset device configuration:** In the **RESET CONFIGURATION** screen, select **Yes** to erase all configuration settings on the device and reboot (installed license files will not be affected), or **No** to cancel.
Serial number	The serial number of the device.

Temperature	Displays the current temperature of the device (**Temperature CPU**) and the SFP modules that are connected, in the temperature unit set in the **PREFERENCES** screen. The temperature preview alternates between the available temperature readings, skipping the SFP ports that are not connected. If the temperature exceeds the safe operating threshold, the temperature icon and reading display in bright red. The safe operating threshold is 80 degrees Celsius for the CPU, and 85 degrees Celsius for commercial SFP modules. (Industrial grade SFP modules could have a higher threshold temperature.) **NOTE**: From the **Temperature unit** field in the **PREFERENCES** screen, you can set **Celsius** or **Fahrenheit** as your choice of temperature display unit for the entire web user interface. You can access the **PREFERENCES** screen by clicking the user initials icon on the top right of the user interface and selecting **Preferences**. Like the other preference settings, the **Temperature unit** selected is stored in your browser cache for a particular device. This information will not be carried over to a different browser. So, each device can have its own preferences settings for a given browser.
Software version	The current software version of the device.
Time	Displays the current time on the device.
Audio stream	Rx • **Connected:** Displays **Connected** when there is an audio stream connected. • **Not connected:** Displays **Not connected** when there is no audio stream. Tx • **Streaming:** Displays **Streaming** when there is audio being streamed. • **Not connected:** Displays **Not connected** when there is no audio stream. When the stream is encrypted, a shield image displays beside the **Connected** or **Streaming** text.

Video stream	Rx • **Connected:** Displays **Connected** when there is a video stream connected. • **Not connected:** Displays **Not connected** when there is no video stream connected. Tx • **Streaming:** Displays **Streaming** when there is video being streamed. • **Not connected:** Displays **Not connected** when there is no video stream. When the stream is encrypted, a shield image displays beside the **Connected** or **Streaming** text.
USB	Rx • **Connected:** Displays **Connected** (routed to OSD) when there is a USB connection. • **Not connected:** Displays **Not connected** when there is no USB connection. Tx • **Streaming:** Displays **Streaming** when USB signal is streamed. • **Not connected:** Displays **Not connected** when there is no USB signal being streamed. When the stream is encrypted, a shield image displays beside the **Connected** or **Streaming** text.
NMOS server status	Displays the NMOS server status. • **Connected:** Displays **Connected** when connected to an NMOS server. • **Not connected:** Displays **Not connected** when it is not connected to an NMOS server.
PTP status	Displays whether it is locked or not locked to the leader, follower, BMC, or disabled. For more information, see "*Time*" on page *50*.
NTP status	Displays whether it is synchronized or not. For more information, see "*Time*" on page *50*.

Streaming bitrate	The current bit rate being streamed. This depends on the codec being used and the speed rating of the SFP module. For more information, see *Streaming* settings.

Switching between the Avio 2 operation modes

Your Matrox Avio2 device can be configured as a transmitter or receiver. It is configured as a receiver by default. At initial boot-up, or after a factory reset, the device boots up in receiver mode. An administrator can change the operational mode of the device.

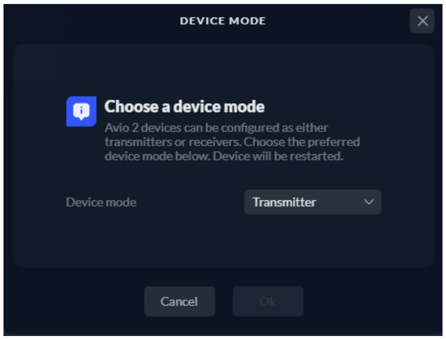
Switch between the device modes

To change the mode from receiver to transmitter (or vice versa):

Step 1. Log in as an Admin user.

Step 2. From the **PROPERTIES** section on the top right, click the **Device** button and select the **Device mode** option.

Step 3. In the **DEVICE MODE** selection screen, select **Transmitter** (or **Receiver)** from the **Device mode** drop-down list.



DEVICE MODE

Choose a device mode

Avio 2 devices can be configured as either transmitters or receivers. Choose the preferred device mode below. Device will be restarted.

Device mode: Transmitter

Step 4. Click **OK**. The **Reboot device** option displays on the top right of the screen.

Step 5. Reboot the device for the change to take place.

Result of this task: The operation mode is switched from receiver to transmitter, or from transmitter to receiver as the case may be.

NOTE The change will not take effect until you reboot the device.

Reboot device

To reboot the device:

Step 1. Log in as an Admin.

Step 2. From the **PROPERTIES** section on the top right, click the **Device** button and select the **Reboot** option from the drop-down list.

Step 3. Click **Yes** in the **REBOOT** confirmation screen that displays.

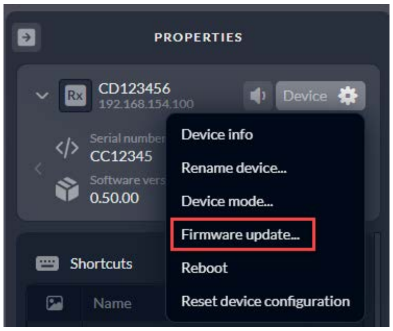
Result of this task: Your device is rebooted.

Firmware update

To update your Avio 2 device firmware:

Step 1. Log in as an Admin user.

Step 2. From the **PROPERTIES** section on the top right, click the **Device** button and select the **Firmware update** option. The **UPDATE FIRMWARE** screen displays. The current firmware version is displayed in the **Current version** field.



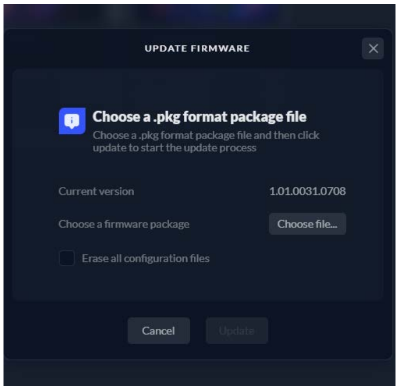
PROPERTIES

CD123456
192.168.154.100

Serial number
CC12345

Software vers
0.50.00

Step 3. In the **Choose a firmware package** field, click the **Choose file** button and select the **.pkg** file corresponding to the firmware version you would like to upgrade to.



UPDATE FIRMWARE

Choose a .pkg format package file
Choose a .pkg format package file and then click update to start the update process

Current version 1.01.0031.0708

Choose a firmware package

□ Erase all configuration files

Step 4. Click **Open**. The package version displays below the **Choose a firmware package** field. The **Erase all configuration files** option also displays now.

Step 5. If you would like to do a full configuration reset, select the **Erase all configuration files** option.

Step 6. Click the **Update** button. The firmware will be uploaded and you can see the update status on the screen.

Step 7. Once the update process is complete, the device will restart. You can then log in from the **WELCOME** screen. **NOTE**: If you erased all your configuration files by selecting the **Erase all configuration files** option earlier, you will need to create a new local admin user account first. In the **WELCOME** screen, click the **Sign up** button to start creating the account. Follow the screen prompts.

For more information on creating the account, see "*Create the first admin user account*" on page *68*.

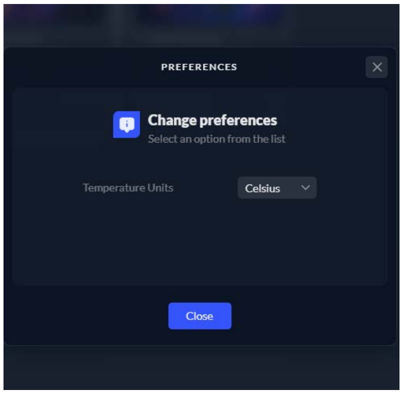
Step 8. Once you are logged in, verify the software version that displays in the PROPERTIES panel on the right.

Result of this task: The device firmware is updated.

NOTE You can also update your Avio 2 firmware using the Matrox Unified Utility. For more information, see "*About the Matrox Unified Utility*" on page *6*.

Preferences

You can set or change your preferred temperature unit to display throughout the web user interface using the **Preferences** option. You can also make your keyboard selection here.



Temperature Units Celsius

The preferences you set are stored in your browser cache for a particular device. These will not be carried over to a different browser. So, each device can have its own preferences settings for a given browser.

Temperature unit

To set your preferred temperature unit:

Step 1. Click your login user initials icon on the top right of the user interface.

Step 2. Select **Preferences**. The **PREFERENCES** screen displays.

Step 3. In the **Temperature unit** drop-down, select **Celsius** or **Fahrenheit**.

Step 4. Click **Save**.

Result of this task: Your preferred temperature display unit for the entire user interface is set.

Keyboard layout

To set your preferred keyboard setting:

Step 1. Click your login user initials icon on the top right of the user interface.

Step 2. Select **Preferences**. The **PREFERENCES** screen displays.

Step 3. In the **Keyboard layout** drop-down, make your selection (default is **en-US**).

Step 4. Click **Save**.

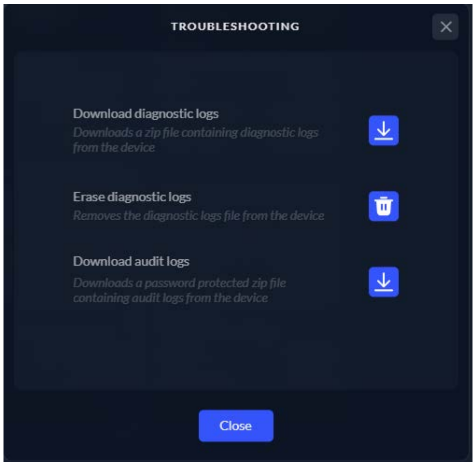
Result of this task: Your preferred keyboard layout is set.

Troubleshooting

To help you to troubleshoot, Avio2 provides two types of log files.

- **Diagnostic logs**: These can help developers to diagnose issues. Diagnostic logs can be deleted from the device.
- **Audit logs**: These provide a detailed audit trail of the operations performed on the device. For security reasons, audit logs cannot be deleted.

An administrator will be able to download these two log files.



Download diagnostic logs

Downloads a zip file containing diagnostic logs from the device

Erase diagnostic logs

Removes the diagnostic logs file from the device

Download audit logs

Downloads a password protected zip file containing audit logs from the device

Download diagnostic logs

To download diagnostic logs:

Step 1. Click your login user initials icon on the top right of the user interface.

Step 2. Select **Troubleshooting**. The **TROUBLESHOOTING** screen displays.

Step 3. Click the download button beside **Download diagnostic logs**.

Result of this task: A zip file with the diagnostic logs is generated and downloaded to your browser's file download location. The zip file is password protected (you need to contact Matrox to get the password). You can delete this file from the device by clicking the button beside **Erase diagnostic logs**.

Download audit logs

To download audit logs:

Step 1. Click your login user initials icon on the top right of the user interface.

Step 2. Select **Troubleshooting**. The **TROUBLESHOOTING** screen displays.

Step 3. Click the download button beside **Download audit logs**.

Step 4. Enter a password between 6 to 64 alpha numeric characters in the **Password** field to protect the audit file that will be generated with the logs. Until you enter a password in the valid format, the download button will remain disabled.

Step 5. Click the download button.

Result of this task: A zip file with the audit logs is generated and downloaded to your browser's file download location. The zip file is password protected.

CHAPTER 3

Using Avio 2

This chapter includes the following topics:

- *Admin tasks (Tx and Rx)*
- *Non-admin user tasks (Rx)*

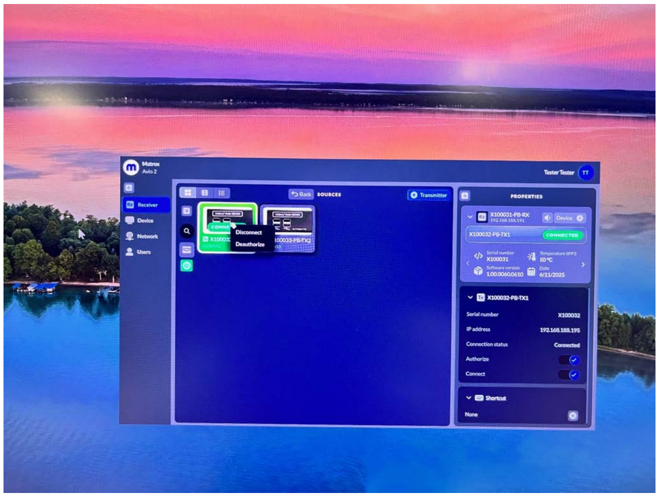
Admin tasks (Tx and Rx)

Once the Administrator completes the initial configuration tasks, the admins and non-admin users (typically operators) can start performing their tasks.

The following are some of the tasks that an admin user can perform using either the web or OSD user interface:

- Tx - Set the Transmitter, Device, Network, and Users settings. For more information, see "*Transmitter settings*" on page *74*.
- Rx - Set the Receiver, Device, Network, and Users settings. For more information, see "*Receiver settings*" on page *33*.
- Reboot, reset device configuration, or rename a device - From the **PROPERTIES** section on the right, click **Device** and select the relevant option.
- Set temperature unit and keyboard preference - Click the log-in section on the top right and select the **Preferences** option.
- See the device information - From the **PROPERTIES** section on the right, click **Device** and select **Info**.

NOTE The information and options that the user can see and set are the same in the web as well as the OSD user interface.



X100031-PB-RX
192.168.188.191

X100032-PB-TX1 CONNECTED

Serial number X100031

Temperature SFP2 50 °C

Software version 1.00.0060.0610

Date 6/11/2025

X100032-PB-TX1

Serial number	X100032
IP address	192.168.188.195
Connection status	Connected
Authorize	✓
Connect	✓

Shortcut

None

Non-admin user tasks (Rx)

Once the Administrator completes the initial configuration tasks, the non-admin users (typically operators) can start performing their tasks.

Using either the web or OSD user interface, non-admin users can:

- Connect to authorized transmitters - **Web user interface**: For more information, see "*Connect the receiver to a transmitter*" on page *38*. **OSD user interface**: There are three ways you can do this. From the **SOURCES** screen, right-click on a transmitter tile and select **Connect**, or double-click the transmitter tile. Or, click a transmitter tile and from the right panel, enable the **Connect** toggle button. For more information, see "*Connect to an authorized transmitter (OSD)*" on page *31*.
- Disconnect from a transmitter - **OSD or web interface**: From the **SOURCES** screen, right-click on a connected transmitter tile and select **Disconnect**, or double-click the transmitter tile. Or, click a connected transmitter tile and from the right panel, disable the **Connect** toggle button. For more information, see "*Disconnect from a transmitter (OSD)*" on page *31*.
- Switch between transmitters - **OSD or web interface**: Right-click from the target transmitter tile and select **Connect**. The connection with the current transmitter gets disconnected and you will get connected to the new transmitter.
- Set temperature unit preference - **OSD or web interface**: Click the log-in circular icon on the top right and select the **Preferences** option.
- Set keyboard layout preference - **OSD or web interface**: Click the log-in circular icon on the top right and select the **Preferences** option.
- See the device information - **OSD or web interface**: From the **PROPERTIES** section on the right, click **Device** and select **Info**.

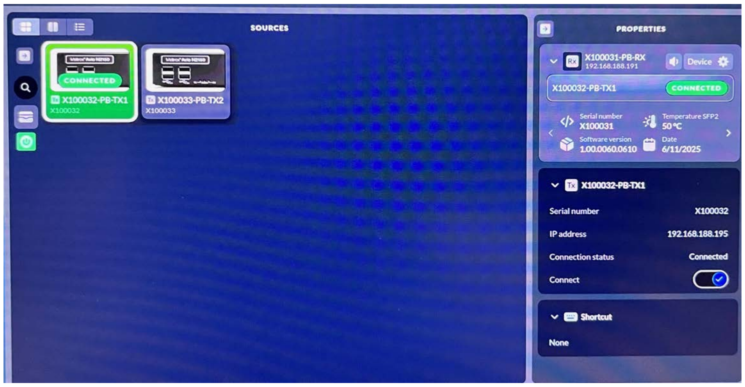
NOTE The information and options that the user can see and set are the same in the web as well as the OSD user interface.

Connect to an authorized transmitter (OSD)

To connect to an authorized transmitter:

Step 1. From the **SOURCES** screen, click the transmitter tile. **NOTE**: You will see all the transmitters on the network that you are authorized to connect with.

Step 2. Right-click the tile and select **Connect**, or double-click on the transmitter tile. Or, from the right panel, enable the **Connect** toggle button.



Rx X100031-PB-RX
192.168.188.191

X100032-PB-TX1 CONNECTED

Serial number X100031
Temperature SFP2 50 °C
Software version 1.00.0060.0610
Date 6/11/2025

Tx X100032-PB-TX1

Serial number X100032
IP address 192.168.188.195
Connection status Connected
Connect ✓

Shortcut

None

Result of this task: You are connected to the transmitter and the content displays on the monitor.

Disconnect from a transmitter (OSD)

To disconnect from a transmitter you are currently connected to:

Step 1. From the **SOURCES** screen, click the transmitter tile.

Step 2. Right-click the tile and select **Disconnect**. Or, from the right panel, disable the **Connect** toggle button. Click **Yes** in the confirmation screen that displays. Or, double click on the transmitter tile.

Result of this task: You are disconnected from the transmitter and the source content disappears from the monitor.

CHAPTER 4

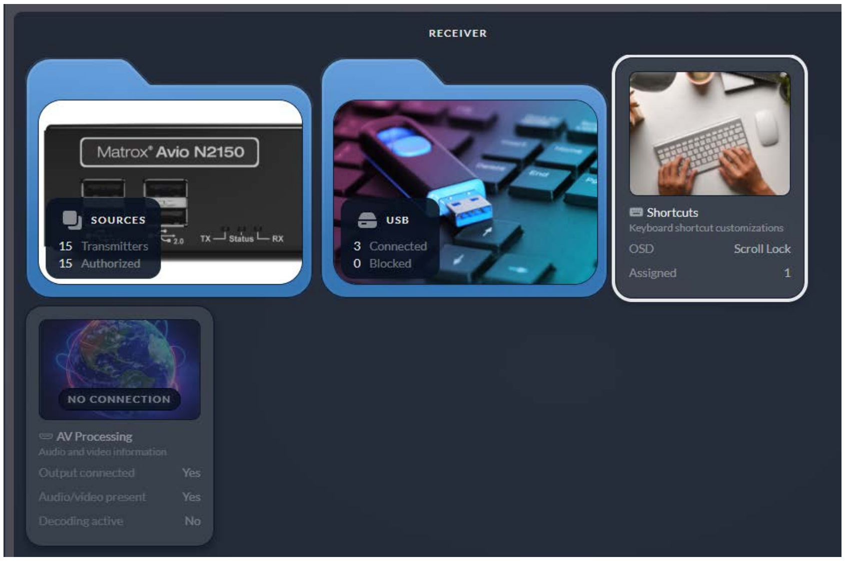
Matrox Avio 2 Receiver settings

This chapter includes the following topics:

Receiver settings

You can manage the sources, USB, and shortcuts for the receiver from the **Receiver** page.

NOTE Only an admin user can set, change, or edit the settings on a receiver. A regular (non-admin) user will have access to very limited options such as connecting to authorized transmitters, viewing device information, and setting temperature unit display preferences.



SOURCES
15 Transmitters
15 Authorized

USB
3 Connected
0 Blocked

Shortcuts
Keyboard shortcut customizations
OSD Scroll Lock
Assigned 1

AV Processing
Audio and video information
Output connected Yes
Audio/video present Yes
Decoding active No

Sources

An Avio 2 receiver connects to sources (Avio 2 transmitters).

From the **Receiver** page, you can view, filter, and manage the sources.

Setting	Description
Sources	
Total transmitters	The total number of available transmitters.
Total authorized	The total number of authorized transmitters.
Connected transmitter	The name of the transmitter to which the receiver is connected.

Folders	
(Custom folder names)	The custom folders created that display here can be used to filter the sources to be displayed.
SOURCES screen (right panel)	
Transmitter's name	The name of the selected transmitter.
Serial number	The serial number of the selected transmitter.
IP address	The IP address of the transmitter's network interface where the control traffic is handled.
Connection status	One of the following displays: • **Connected:** Displays **Connected** when the receiver is connected to the transmitter. • **Not connected:** Displays **Not connected** when the receiver is not connected to the transmitter.
Authorize	Following are the options: • **Enable:** Toggle to authorize the transmitter for the receiver. • **Disable:** Toggle to de-authorize the transmitter for the receiver.
Connect	Following are the options: • **Enable:** Toggle to connect to the transmitter. • **Disable:** Toggle to disconnect from the transmitter.
Shortcut	The shortcut keys for the selected transmitter. If there is none specified for the selected transmitter, you can assign the shortcut by clicking on the (+) plus icon. In the **SHORTCUTS** screen, using the keyboard, select the key combination to be assigned for the shortcut in the **Key combination** field.
SOURCES screen	

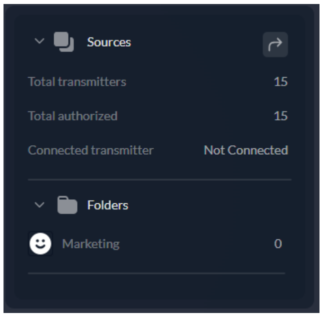
+Transmitter button	Click the button to add a transmitter from the **ADD TRANSMITTERS** screen.
...	**Add folder**: Click to display the **ADD FOLDER** screen from where you can add a new folder. Enter the folder name in the **Name** field and from the **Image** field, click the **Upload** button and select an image to be associated with the folder. You can use folders to organize transmitters into them and later use these folders to filter (by using the **Custom folder** option). For more information, see "*Add transmitters to a folder*" on page *37*
Filters	On a Receiver, discovered Transmitter devices can be filtered. • **Show all:** Display all the discovered transmitters. This is the default view. • **Connected:** Display only the transmitters that the receiver is connected to. • **Custom folder:** Click on a custom folder to display only the transmitters clubbed into the folder.
ADD TRANSMITTERS screen	
Filters	Following are the filter options: • **Show all:** Display all the discovered transmitters. This is the default view. • **Available:** Use this filter to hide the already authorized transmitters. • **Authorized:** Only transmitters that are discovered and authorized will display when you select the **Authorized** filter.
Cancel / Save button	Following are the button options: • **Cancel:** Click **Cancel** to discard your changes. • **Save:** Click **Save** to save the changes you made.

Access the sources list

To access the list of sources:

Step 1. From the left navigation menu, select **Receiver**.

Step 2. Click the **Sources** tab. You will see a summary on the right with the total number of available transmitters and the total number of authorized transmitters.



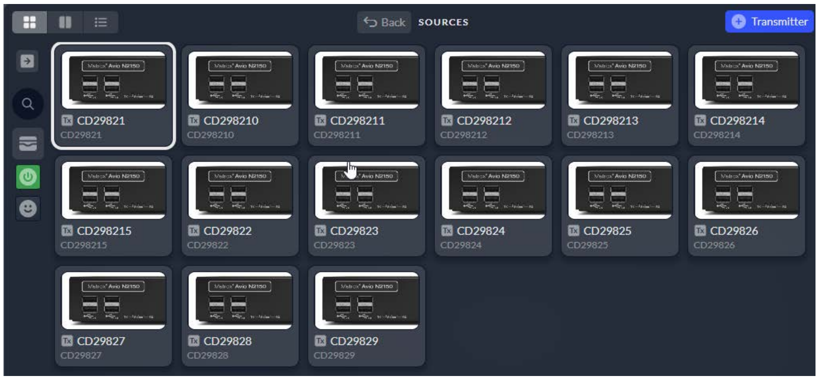
Sources

Total transmitters	15
Total authorized	15
Connected transmitter	Not Connected

Folders

Marketing	0

Step 3. You can now double-click the tab, or click the right arrow icon (↪) that displays when you hover over the **Sources** tab. The **SOURCES** page with a list of transmitters and options to filter them displays.



Result of this task: The default view lists the device tiles with the device name and serial number. When you click on a device tile, the Serial number, IP address, Connection status, Authorize, and Connect fields display details for the selected device in the right panel. The shortcut keys associated to the device are shown under **Shortcut**.

When done, remember: You have the option to filter and view the devices in the list in many ways. To see the connection status, IP address and the shortcut associated with each device on the device tile itself, select the tile (▥) filter icon. To see the same details in a tabular form, click the table (☰)filter icon.

NOTE By default, all the transmitters are displayed (**Show all** filter) in the list. To see only the connected transmitters, click the **Connected** filter.

Add a folder

You can add a folder to organize or group transmitters into it for easy filtering.

To add a folder:

Step 1. From the left navigation menu, select **Receiver**.

Step 2. Click the **Sources** tab.

Step 3. You can now double-click the tab, or click the right arrow icon (↱) that displays when you hover over the **Sources** tab. The **SOURCES** page displays.

Step 4. Click the **right arrow** icon (→) to the left of the page to expand the filters.

Step 5. Click the more icon (⋯) to access the **Add folder**, **Edit** and **Delete** options.

Step 6. Click the **Add folder** option. The **ADD FOLDER** screen displays.

Step 7. In the **Name** field, enter a name for your new folder.

Step 8. In the **Image** field click the **Upload** button to upload an image that will be associated with the folder.

Step 9. Click **OK**.

Result of this task: The new folder is added and displays in the filter list.

Add transmitters to a folder

You can add transmitters that belong to a logical group into a folder.

To add transmitters to a folder:

Step 1. From the left navigation menu, select **Receiver**.

Step 2. Click the **Sources** tab.

Step 3. You can now double-click the tab, or click the right arrow icon (↱) that displays when you hover over the **Sources** tab. The **SOURCES** page displays.

Step 4. Click the **right arrow** icon (→) to the left of the page to expand the filters.

Step 5. Drag and drop a device to the folder. Repeat till you have added all the transmitters you want to be included in the folder. **NOTE**: You can select multiple transmitters by holding the **Ctrl** key and clicking on the device tiles. Alternatively, you can right-click a device tile, select the **Assign to folder** option, then choose the folder to which you want to add the transmitter.

Result of this task: The image associated with the folder now displays on the device tile of all the transmitters in the group. The folder displays the number of transmitters that have been added to the folder.

When done, remember: To remove the transmitter from the folder, right-click the device tile, select the **Assign to folder** option, then choose **None**.

NOTE A transmitter can be added to only one group.

Authorize a source (transmitter)

An admin user can authorize a transmitter.

To authorize a transmitter for the receiver:

Step 1. From the left navigation menu, select **Receiver**.

Step 2. Click the **Sources** tab.

Step 3. You can now double-click the tab, or click the right arrow icon (↱) that displays when you hover over the **Sources** tab. The **SOURCES** page displays.

Step 4. Click the **Transmitter** button (Transmi)on top of the page. The **ADD TRANSMITTERS** screen displays.

Step 5. Click the **Available** filter.

Step 6. Right-click the device tile of the transmitter you want to add and select **Authorize**, or double-click the device tile. Or, click the device tile and toggle the **Authorize** button in the panel to the right.

Step 7. Click **Save**.

Result of this task: The transmitter is now an authorized source for the receiver and the transmitter device tile displays in the **SOURCES** page.

When done, remember: You can de-authorize a transmitter by right-clicking the device tile from the **SOURCES** page and selecting the **Deauthorize** option, or by double-clicking the tile, or by clicking the tile and toggling the **Authorize** button in the panel to the right.

NOTE Only an admin user will be able to do this task.

Connect the receiver to a transmitter

Both admins and users can connect to a transmitter from a receiver.

To connect the receiver to a transmitter:

Step 1. From the left navigation menu, select **Receiver**.

Step 2. Click the **Sources** tab.

Step 3. You can now double-click the tab, or click the right arrow icon (↱) that displays when you hover over the **Sources** tab. The **SOURCES** page displays.

Step 4. Right-click the device tile of the transmitter you want to connect to and select **Connect**, or double-click the device tile. Alternatively, you can click the device tile, then toggle the **Connect** button on the right panel.

Step 5. Click **OK** in the **CONNECTION** page that displays the “Confirm connection change” message.

Step 6. Click **Save**.

Result of this task: The receiver is connected to the transmitter.

When done, remember: You can disconnect the transmitter by right-clicking the device tile from the **SOURCES** page and selecting the **Disconnect** option, or by double-clicking the device tile, or toggling the **Connect** button on the right panel.

NOTES

- If the receiver was connected to a transmitter before you made the change, the receiver will disconnect from the previous transmitter and connect to the new transmitter.
- When either the video resolution or refresh rate is different between the previous transmitter and the current transmitter, the monitor attached to the receiver will take some time to adapt to the change in video mode (a video mode being the combination of resolution with refresh rate). Some monitors could take significantly longer than others.
- When the transmitter starts streaming for the first time after booting, it could take a few seconds, whereas it takes only a fraction of a second during subsequent disconnects and reconnects (for a multicast stream). For a unicast stream, the delay you see on a first connection is also experienced in subsequent connections.
- When a transmitter's encoding setting changes, say from compressed to uncompressed, or from one codec to another (such as ProAV, JPEG-XS), the transmitter could have a delay of a few seconds.

USB

From this section, you can manage the USB settings.

USB device families

Specific types of USB devices are grouped into families so an administrator can easily control how an Avio 2 receiver behaves when a new USB device is plugged into one of the front USB ports.

Each family has a corresponding tab associated with it. Selecting this tab will show the family properties in the right panel of the screen.

The USB families are:

- Mouse and keyboards
- Storage devices - This includes USB keys and external hard drives and solid state drives (SSDs)
- Audio devices (USB audio devices only)
- Tablets and touchscreens
- Other - This includes any USB device not covered in the families above, such as joysticks and any HID device

Set the default rule for a USB family

For each USB family, as an administrator you can select one of two rules: either **Allow** or **Block**.

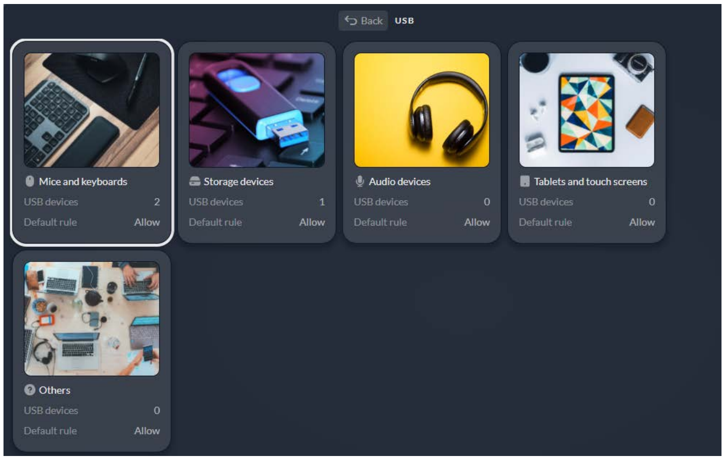
This is done by changing the selection in the family drop-down under the name of the family in the properties panel.

The default rule of **Allow** or **Block** you set will be followed when any new USB device is connected to the receiver in the future.

To set the default rule for a USB family:

Step 1. When logged in as an admin, from the left navigation menu, select **Receiver**.

Step 2. Double-click the **USB** tab or click the right arrow icon (↱) that displays when you hover over the **USB** tab. The **USB** page displays with a tab for each USB family.



Mice and keyboards
USB devices 2
Default rule Allow

Storage devices
USB devices 1
Default rule Allow

Audio devices
USB devices 0
Default rule Allow

Tablets and touch screens
USB devices 0
Default rule Allow

Others
USB devices 0
Default rule Allow

Step 3. Click the USB family tab for which you would like to set the default USB connection rule, and from the **Default USB rule** field in the right panel, select **Allow** or **Block** from the drop-down list. **NOTE**: The default option is **Allow**.

Result of this task: The default USB connection rule is set. The next time a USB device from the USB family is connected to the receiver, depending on the rule you set here, the connection will be allowed or blocked. If you select **Block**, each USB device of the corresponding family is ignored by the receiver and no USB channel is created between the device and the transmitter to which the receiver is connected (and thus not connected to the source PC). If you select **Allow**, when connecting the receiver to a transmitter, each USB device of the corresponding family is sent to the attached transmitter (and thus its attached source PC) and can be used as if it is connected to the source PC directly. When a new USB device of the corresponding family is plugged into the receiver while the receiver is already connected to a transmitter, this new USB device is sent to the attached transmitter (and thus its attached source PC) and can be used as if it was connected to the source PC directly.

When done, remember: You can repeat this task for the other USB families as required.

NOTES

- You need to be logged in as an admin to be able to do this task.
- The default USB rule for a USB family can be overridden for a specific USB device by toggling the button that displays beside the USB device. For example, if you have blocked Storage devices, you can still allow a particular storage device by toggling the button to the allow position (blue tick). The USB device will be connected at the time you save the override setting.

Shortcuts

You can assign shortcut keys to quickly access the OSD and transmitters.

Setting	Description
Shortcuts	
Name	Name of the OSD or transmitter.
More button (...)	Following are the options: • **Reset:** Erases the shortcut keys set for the OSD or transmitter. • **Change:** Set the shortcut key combination for the OSD or transmitter. The default shortcut key for the OSD screen is **Scroll lock**. You can change this if required.
SHORTCUTS screen	
Key combination	Enter the shortcut key combination in this field.

Set the shortcut keys

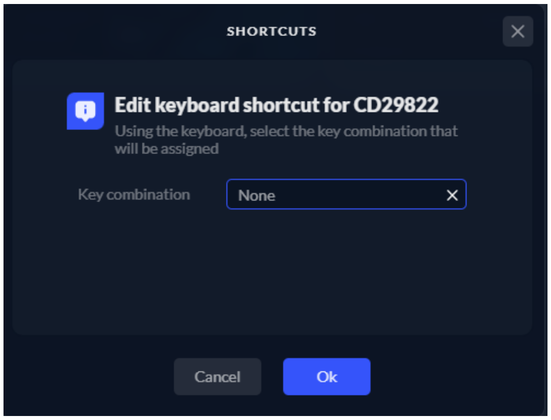
To set (or change) the shortcut keys:

Step 1. When logged in as an admin, from the left navigation menu, select **Receiver**.

Step 2. Click the **Shortcuts** tab. The **Shortcuts** section displays on the right panel with a list of the OSD and transmitters available. **NOTE**: The default shortcut key for the OSD is **Scroll lock**. You can change this if necessary.

Step 3. Click the more button (**...**) beside the transmitter (or OSD) for which you want to set (or change) the shortcut keys and select **Change**.

Step 4. In the **SHORTCUTS** screen that displays, enter the shortcut keys combination in the **Key combination** field.



SHORTCUTS

Edit keyboard shortcut for CD29822

Using the keyboard, select the key combination that will be assigned

Key combination: None

Step 5. Click **OK**.

Step 6. Repeat steps 3 to 5 for the rest of the transmitters.

Result of this task: The shortcut keys are set for the transmitters and/or the OSD.

When done, remember: You can remove the associated shortcut keys for a transmitter or OSD by clicking on the more button (**...**) and selecting the **Reset** option.

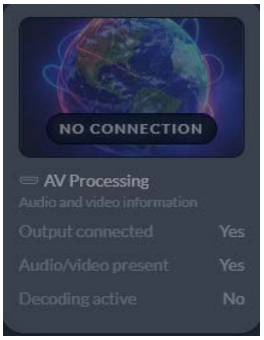
NOTE Only an admin user will be able to do this task.

AV processing

You can see the audio and video processing information from this section.

When an Avio 2 receiver has an established connection with a transmitter and the video content is transmitted over the network, the audio and video stream details are displayed on the **AV Processing** tile.

When the receiver does not have an established connection with the source, the **AV Processing** tile displays in a disabled state with the message **NO CONNECTION**.



NO CONNECTION

AV Processing

Audio and video information

Output connected	Yes
Audio/video present	Yes
Decoding active	No

The tile also displays the following information.

Field	Description
AV Processing (Rx)	
Output connected	Displays **Yes** when the output is connected, otherwise **No**.
Audio/Video present	Displays **Yes** when audio/video stream is available, otherwise **No**.
Decoding active	Displays **Yes** when decoding, otherwise **No**.

When the receiver has an active connection with a transmitter, the tile displays **CONNECTED**. When you click on the tile, you can see the stream details for both audio and video in the right panel.

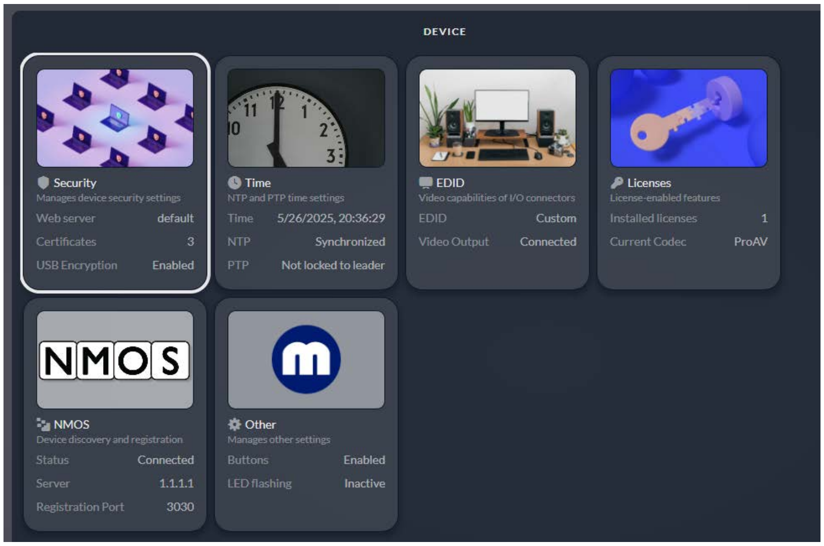
Field	Description
Video stream	
Stream label	The stream label displays the device name appended with "Video Receiver" followed by a number.
Resolution	Displays the resolution and frame rate of the stream.
Bit depth	Displays the bit depth of the stream.
Scaling	Displays the scaling when the stream is scaled, otherwise displays **No scaling**.
Compression type	Following are the compression type options: • JPEG XS • Pro-AV
Encryption	Displays **Active** when the video stream in encrypted, otherwise **Inactive**.
Audio stream	
Stream label	The stream label displays the device name appended with "Audio Receiver" followed by a number.

Audio format	Displays the audio stream format.
Encryption	Displays **Active** when the audio stream in encrypted, otherwise **Inactive**.

Device settings

From here, you can set and manage the settings related to the device.

NOTE The device settings options are similar for the receiver and the transmitter, with minor differences.



DEVICE

Security
Manages device security settings
Web server: default
Certificates: 3
USB Encryption: Enabled

Time
NTP and PTP time settings
Time: 5/26/2025, 20:36:29
NTP: Synchronized
PTP: Not locked to leader

EDID
Video capabilities of I/O connectors
EDID: Custom
Video Output: Connected

Licenses
License-enabled features
Installed licenses: 1
Current Codec: ProAV

NMOS
Device discovery and registration
Status: Connected
Server: 1.1.1.1
Registration Port: 3030

Other
Manages other settings
Buttons: Enabled
LED flashing: Inactive

Security

Matrox Avio 2 uses various certificates and encryption to provide security to its operations.

NOTES

- Only an administrator can modify the certificate settings.
- Avio 2's default certificates are internal self-signed certificates, signed with a Matrox CA (certified authority). Since this Matrox CA is not in the trusted store of the browser, they are flagged as insecure by all web browsers. When accessing Avio 2's web UI for the first time after a factory reset, or from a new browser, you may encounter an warning "*Your connection is not private*". You can ignore this warning and click the "Proceed to [IP address] (unsafe)" link to proceed to the website. Subsequently, you can either install the Matrox CA in your browser's trusted store, or deploy your own certificate on the Avio 2 device.
- You cannot remove Avio 2's default certificates. If you deploy and use custom certificates, they are erased during a configuration or factory reset. In this case, the default certificates will be used.

Certificates used must meet the X.509 specification. The two supported certificate usages are Web Server and Certificate Authorities.

- **Web Server certificate** - This is used when serving the Web UI and the OSD web pages. The Web Server certificate has to be provided with its private key.
- **Certificate Authorities** - This is a list of public certificates that the device recognizes as certificate authorities in the PKI Infrastructure.

Setting	Description
Certificates	
Web server	This is used for the Web UI and the OSD web pages. The Web Server certificate has to be provided with its private key.
Certificate used	The Web server certificate that is used. Default RSA and Default EC are used for maximum compatibility.
Certificates	The Web server certificates available. This displays the installed certificates with a private key, listed by user-defined labels.
Trusted CA	This displays a list of public certificates that the device recognizes as certificate authorities in the PKI Infrastructure.
Encryption	
Pre-shared keys	To ensure privacy of the connection between a receiver and a transmitter, the audio, video, and USB streams are, by default, encrypted. When a stream is encrypted, it is referred to as being protected. Encryption of the audio and video streams can be disabled, but not the USB stream as it needs to be always encrypted.

Plus button (+)	Click the plus button (+) to create a new key and ID pair. You can have up to four (4) key and ID pairs. **NOTE**: Key and ID pairs are stored by operational mode. When switching between Rx and Tx operation mode, the key assignment you had set to perform encryption is lost. You need to reselect which key has to be used to encrypt the audio and video. Since USB must always be encrypted, when switching the operation mode from Tx to Rx, the first encryption key in the list is automatically assigned to encrypt the USB stream. When switching from Rx to Tx, the audio and video streams will get encrypted only after you reselect which key to use to encrypt the audio and video. For more information see "*Add an encryption key and ID pair*" on page 49.

More button (...)	To associate a key and ID pair with a stream that needs to be protected (encrypted), click the more button (...) and select the **Protect USB** (Rx only), **Protect Audio** (Tx only), or **Protect Video** (Tx only) option. A key and ID pair can be deleted by clicking the more button (...) and selecting **Delete**. **NOTE**: Any stream protected using this key and ID pair that is deleted will no longer be protected. To unencrypt an audio stream, click the more button and select the **Unprotect audio** option. To unencrypt a video stream, click the more button and select the **Unprotect video** option. The same key and ID pair can be used to encrypt multiple streams. Click the more button (...) and select the protect option for the different stream types you would like to encrypt. **NOTE**: You can make changes to the stream encryption settings only while the device is not connected. You can delete a key and ID pair only when it is not assigned to protect a stream. To delete a key and ID pair that is currently being used to protect a stream, first choose **Unprotect** from the menu, then delete the key. Or, choose **Protect** from the menu of another key so that the current key is no longer used to protect that stream.

Upload a Web Server certificate

To upload a Web Server certificate:

Step 1. From the left navigation menu, select **Device**.

Step 2. Click the **Security** tab.

Step 3. For a Web Server, from the **Certificates** tab on the right, beside **Certificates**, click the plus icon. The **ADD CERTIFICATE** screen displays.

Step 4. Enter a name for the certificate in the **Name** field.

Step 5. Click the **Choose file** button and select a file from the file selection page that opens.

Step 6. Click the **Choose private key** button and select a file from the file selection page that opens.

Step 7. Click **Save**.

Result of this task: The certificate is uploaded to the device and displays in the **Certificates** section. The expiry date of the certificate is also displayed.

When done, remember: You can view the details, export, or delete the certificate by using the more (...) button to the right of the certificate. **NOTE**: Any private key uploaded with the certificate can’t be exported.

NOTE After you upload a certificate, you must select it from the Web server > Certificate used setting. Otherwise, it will not be used and the previous certificate used for the web server will continue to be used. Expired certificates will display **Expired on** in red text.

Upload a Certificate Authority certificate

To upload a Certificate Authorities certificate:

Step 1. From the left navigation menu, select **Device**.

Step 2. Click the **Security** tab.

Step 3. For a Certificate Authority, from the **Certificates** tab on the right, beside **Trusted CA**, click the plus (+) icon.The **ADD CERTIFICATE** screen displays.

Step 4. Enter a name for the certificate in the **Name** field.

Step 5. Click the **Choose file** button and select a file from the file selection page that opens.

Step 6. Click **Save**.

Result of this task: The certificate is uploaded to the device and displays in the **Certificates** section under **Trusted CA**. The expiry date of the certificate is also displayed.

When done, remember: You can view the details, export, or delete the certificate by using the more (...) button to the right of the certificate.

NOTE Expired certificates will display **Expired on** in red text.

Add an encryption key and ID pair

To add an encryption key and ID pair:

Step 1. From the left navigation menu, select **Device**.

Step 2. Click the **Security** tile.

Step 3. From the Encryption tab on the right, click the plus button (+) beside Preshared keys.

Step 4. Enter (or paste) the encryption ID in the **ID** field. Enter (or paste) the encryption keys in the **PSK** field.

Step 5. Alternatively, you can click the **Generate** button to generate a new random encryption key and encryption ID.

Step 6. Copy the key and ID pair information to a safe place.

Step 7. Click **Done**. **NOTE**: This doesn’t save the changes to the device yet.

Step 8. Click **Save** to save the changes to the device.

Result of this task: The key and ID pair is uploaded to the device and displays in the **Pre-shared keys** section under the **Encryption** tab.

When done, remember: You can associate a key and ID pair with a stream that needs to be protected.

NOTE Once saved, the encryption keys will no longer be visible in the user interface and can't be extracted from the device.

Time

You can access time settings by selecting **Device** from the left navigation menu, and clicking on the **Time** tab.

Avio 2 supports two different clock synchronization mechanisms:

- **NTP (Network time protocol)** - Allows synchronization accurate within milliseconds. NTP clock synchronization affects all management and USB traffic. When NTP is disabled, the device is considered to be in "free running" clock mode. In this mode, the clock shown on the web UI might drift as time goes by as the device clock-tracking is not an ideal clock.
- **PTP (Precision time protocol)** - Provides control over the use of precision time protocol. Allows synchronization within nanoseconds. PTP clock synchronization affects audio and video traffic.

Setting	Description
Time	
NTP time	You can enable or disable the **NTP time** toggle switch. By default, **NTP time** is enabled. **NOTE**: When transitioning from disabled to enabled, the device time is updated with the actual time of the user's PC before enabling NTP. As PC's clock are usually synchronized with an NTP server, this minimizes the time needed for the device's NTP algorithm to converge with the NTP time source. **NOTE**: When disabling NTP time, the device switches to free-running mode, and the device time is updated with the actual time of the user's PC.
Servers	Enter one or more NTP time servers to use. You can separate multiple server names using space in between. By default, the server list contains **time.matrox.com**.
PTP time	You can enable or disable the **PTP time** toggle switch. **NOTE**: PTP time is supported only on 10G SFP module connections.
Mode	**Follower** - The device will synchronize its PTP clock to the outside clock source as defined by the PTP algorithm part of the PTP specification. **Best Master Clock** - The device will participate in the election of the best clock as defined by the PTP algorithm part of the PTP specification. In this mode, the device could end up being either a follower (as described in the follower mode described above) or the leader (meaning the device's PTP clock is used as the master clock of the PTP domain).

Domain	This is the clock domain number. Enter a value between 0 and 127. Defaults to **127**.
Delay request interval	Enter a value between 0 and 5. Defaults to 1.
Announce interval	Enter a value between 0 and 4. Defaults to 0.
Sync interval	Enter a value between -7 and 1. Defaults to -3.
Priority 1 mode	Select **Automatic** or **Custom**. For Custom, the valid values are between 1 and 255. Defaults to **1**.
Priority 1	Primary priority of the device clock.
Priority 2 mode	Select **Automatic** or **Custom**.
Priority 2	Secondary priority of the device clock. This is available only when the PTP **Mode** is set to **Best Master Clock**. The setting is disabled in the web UI and ignored when the PTP mode is set to **Follower**. Enter a value between 1 and 255. Defaults to **1**.

NOTE You cannot change the date and time of the device manually through the web interface.

EDID

An administrator can manage the EDID (Extended Display Identification Data) for the display connected to the transmitter or receiver device.

Matrox provides separate EDID files for different monitor profiles on the Matrox web site. You need to download the desired EDID from the Matrox web site then use the EDID upload feature in the Avio 2 web UI.

An administrator can do the following tasks:

- Upload an EDID to a Tx - This is done to override the default EDID at the Avio 2 HDMI input. This influences the source PC video mode. An EDID uploaded to a device can later be downloaded from the device.
- Upload an EDID to a Rx or Tx - This is done to override the EDID retrieved from the monitor at the output of an Avio 2 receiver or transmitter. This helps mitigate issues

with the detection of the attached physical monitor (for example, a monitor with a damaged EDID or an unreliable HDMI cable between the Avio 2 receiver or transmitter output and the monitor).

- Download the EDID of a display connected to the Rx or Tx - The EDID currently being used could be the default Avio 2 input EDID, the EDID from the monitor currently attached to the Avio 2 receiver or transmitter output, or an EDID previously uploaded to either the input or the output.

NOTES

- Custom EDIDs - A maximum of two (2) concurrent custom EDIDs can be on the device simultaneously (one for input, and one for output).
- Optimized for UHD - Avio 2 is optimized for UHD resolutions but remains compatible with all other resolutions. In compatibility mode, Avio 2 may continue working in UHD resolution for streaming, whatever the resolution you set in the OS user interface. To circumvent this and achieve optimal behavior for non-UHD resolutions, you need to use an EDID that is provided by Matrox. Matrox provides several EDID files for different resolution and frame rate (23.94 to 60 Hz) combinations.
- High-frequency - High-frequency frame rates (such as 120 Hz) are supported. For setups requiring high refresh rates, it is recommended to use the display’s EDID.
- Modern OS - Modern operating systems like Windows 11 and macOS will always use the highest preferred resolution advertised by a display and apply visual scaling when you select a different resolution. However, the system will continue to run at the highest resolution internally. For more information see "*EDID and modern OS*" on page 54.
- Modify the EDID - Since the Avio 2 EDID advertises 3840x2160p60 as the preferred resolution, this will, in most cases, be the only resolution output by the source. For lower resolutions, this is suboptimal as it results in unnecessary bandwidth usage and potential quality degradation. The only guaranteed way for you to enforce a specific resolution—independent of the GPU or source software—is to modify the EDID.
- Passthrough monitor - A monitor connected to the passthrough output may not work, resulting in a black or non-active screen, if the source is set to a higher or incompatible resolution than what the monitor supports. The passthrough monitor ***must be*** compatible with the resolution provided to the Avio 2 transmitter input. You can also check the source resolutions in the Avio 2 transmitter’s user interface. To ensure that the passthrough monitor works correctly, you need to provide its EDID to the Avio 2 transmitter.

Field	Description
EDID (Tx)	
Input EDID	Displays the **Manufacturer**, **Model**, and the **Preferred mode**. You can upload an input EDID file by using the **Upload** button from **Upload EDID file**.

Output EDID	Displays the **Status** as **Connected** or **Not connected**. You can upload an output EDID file by using the **Upload** button from **Upload EDID file**.

EDID and modern OS

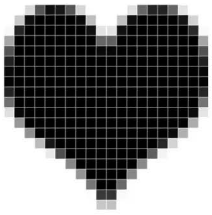
While scaling techniques like Retina Display (on macOS) and Windows Scaling (on Windows 11) improve local rendering quality, they introduce excessive bandwidth consumption and degrade overall image quality in network-based video streaming.

Since the OS continues to output the highest possible resolution, even when the user perceives a lower effective resolution, the actual transmitted signal remains at a higher resolution than necessary, leading to unnecessary bandwidth consumption, reduced image quality, and wasted encoding resources.

To optimize AV-over-IP transmissions to get the best possible quality at an optimal bit rate, it's crucial to force native resolution rendering whenever possible. However, current OS behaviors make this difficult to achieve without manual intervention. You can optimize this by using custom EDIDs.

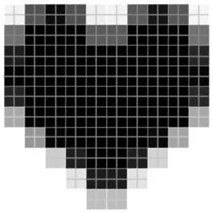
Below is a visual example of the same drawing at the same size (visually) but at different display and transmit resolutions.

(a)



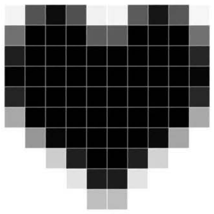
3840x2160 drawing created
for a 3840x2160 display
Visually optimal
4x transmission bitrate over 1920x1080

(b)



1920x1080 drawing created for
a 3840x2160 display
Lower quality but still using
4x transmission bitrate over 1920x1080

(c)

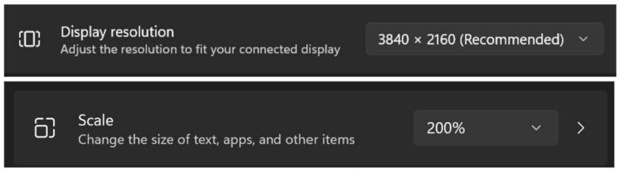


1920x1080 drawing created for
a 1920x1080 display
Lower quality but optimal
for bitrate transmission

In Windows 11, see the Advanced Display Settings panel (go to System > Display > Advanced display).

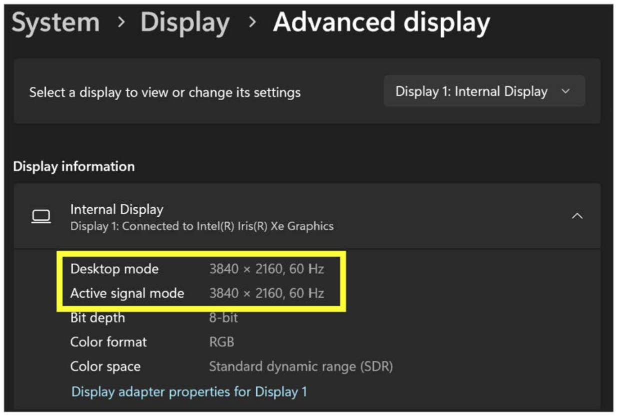
Example A:

Here, the display resolution is set to 3840x2160 with a 200% scaling factor, meaning the effective UI resolution perceived by the user is 1920x1080.



Display resolution
Adjust the resolution to fit your connected display
3840 × 2160 (Recommended)

Scale
Change the size of text, apps, and other items
200%



System › Display › Advanced display

Select a display to view or change its settings
Display 1: Internal Display

Display information

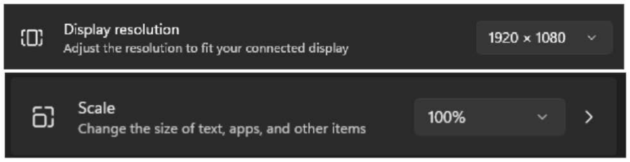
Internal Display
Display 1: Connected to Intel(R) Iris(R) Xe Graphics

Desktop mode	3840 × 2160, 60 Hz
Active signal mode	3840 × 2160, 60 Hz
Bit depth	8-bit
Color format	RGB
Color space	Standard dynamic range (SDR)

Display adapter properties for Display 1

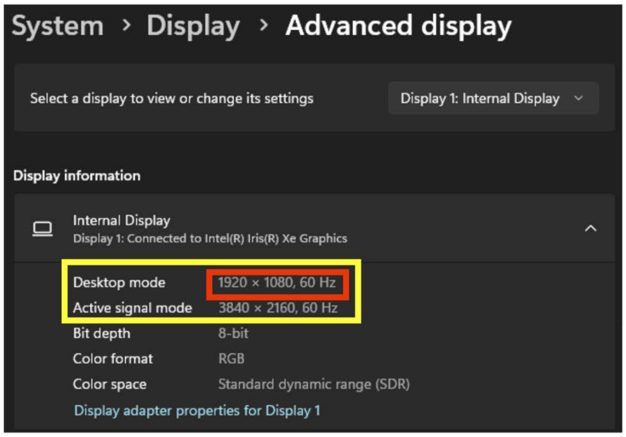
Example B:

Here, the resolution is manually set to 1920x1080 with a 100% scaling factor, resulting in the same visual appearance as Example A.



Display resolution
Adjust the resolution to fit your connected display
1920 × 1080

Scale
Change the size of text, apps, and other items
100%



System › Display › Advanced display

Select a display to view or change its settings
Display 1: Internal Display

Display information

Internal Display
Display 1: Connected to Intel(R) Iris(R) Xe Graphics

Desktop mode	1920 × 1080, 60 Hz
Active signal mode	3840 × 2160, 60 Hz
Bit depth	8-bit
Color format	RGB
Color space	Standard dynamic range (SDR)

Display adapter properties for Display 1

Despite these two configurations looking nearly identical to the viewer, the actual output resolution on the HDMI connector remains at 3840x2160 in both cases. This can be confirmed by checking the Active signal mode in Windows settings, which indicates the true transmission.

Upload the EDID of a Tx or Rx

You can upload custom EDIDs to the device. When you upload an EDID, it overrides the "Default" EDID that is already present.

When a custom EDID is uploaded, users can delete it by pressing the **Delete** button. Upon deletion, the device reverts to its internal default EDID (if any).

To upload the EDID to a device:

Step 1. From the left navigation menu, select **Device**.

Step 2. Click the **EDID** tab.

Step 3. Upload a custom EDID from the **EDID** section on the right by clicking the **Upload** button. **NOTE**: The maximum file size is 30 MB.

Result of this task: The EDID is uploaded to the device. The **Manufacturer**, **Model**, and **Preferred mode** are displayed.

NOTE When you upload an EDID, it overrides any default EDID that is present.

Download the EDID of a display

The EDID currently being used at the input or output of the Avio 2 device can be downloaded to a file.

To download the EDID of a display:

Step 1. From the left navigation menu, select **Device**.

Step 2. Click the **EDID** tab.

Step 3. From the **EDID** section on the right, click the download icon (⤓).

Result of this task: The EDID is downloaded to the default location.

NOTE When you download an EDID file, it will be in the "**Manufacturer_Model_SerialNumber.bin**" format. The original name of the EDID file will not be kept.

Licenses

You can install a license file on a device from here and validate it. A license file could be specific to one or multiple devices. You need a license to unlock the JPEG-XS codec.

NOTE You can install licenses only remotely (not from the OSD).

The **Installed Licenses** section on the right panel displays the licenses that have been installed on the device.

Field	Description
Licenses	
Installed Licenses	Displays the licenses that have been installed on the device. You can upload an input EDID file by using the **Upload** button from **Upload EDID file**.
Codec Settings	The **Codec Settings** section displays only when a JPEG XS license is installed. **Current Codec** - Displays the current codec being used. **Configured Codec** - You can select from **ProAV** and **JPEG XS**.

To install a license:

Step 1. When logged in as Admin, from the left navigation menu, select **Device**.

Step 2. Click the **Licenses** tab.

Step 3. From the **Licenses** section on the right, click the plus (+) icon.

Step 4. Click the **Choose file** button in the **LICENSE** screen and select a **.lic** format license file. **NOTE**: You can upload a single file with a maximum size of 30 MB in each upload. To minimize security risks, the license file you upload is kept in a separate directory outside of other configuration files on the device (in the file path /data/licenses).

Step 5. When installing a JPEG-XS license, select the codec from the drop-down that appears right below license.

Result of this task: The selected license is installed.

When done, remember: When installing a JPEG-XS license, it will immediately be enabled by default, requiring a reboot.

NOTE Once a license file is installed on a device, it cannot be deleted.

NMOS

You can see and define NMOS related settings in this section.

Networked Media Open Specifications (NMOS) allows devices to be discovered through a NMOS registry server. Matrox Avio 2 devices can announce their presence on the network using the NMOS protocol. In addition, Avio 2 receivers can find Avio 2 transmitters on the network using NMOS.

Setting	Description
NMOS (tile)	
NMOS	By default, NMOS is disabled. Toggle the button to enable it.
Status	Displays whether connected, partially connected, or not connected.
Server	The NMOS registry server.
Registration port	The server port number.
Servers (right panel tab)	
Servers	This tab displays the NMOS registry servers found along with the IP address and the NMOS API version supported for each. The server where the device is currently connected displays CONNECTED beside it. If no server is found, “NO NMOS REGISTRY SERVER FOUND” displays.
Node (right panel tab)	
Registered on the server	This displays the status of whether the node was successfully registered to an NMOS registry server or not. When **Yes** displays, it indicates that communication with a NMOS server could be established.
Customize NMOS connector	The network connector used for the NMOS registration to the server.
Override connector	The network connector used for the NMOS registration to the server.
Port	The interface and port which will be used by the device to send its updates to the registry server. The default node port is **5051**.

Registry (right panel tab)	
Discovery method	Select the NMOS registry broadcast settings. When NMOS is enabled, the discovery method is automatic (**MDNS and DNS/SD**). **MDNS and DNS-SD** - This uses DNS-SD first, then mDNS to find a NMOS registry service. Select the API version used in the **API version** field. Defaults to **v1.3**. For manual selection, specify the corresponding settings. **MDNS** - Use this if the NMOS registry service is advertised on the network via mDNS (Domain Name Service over link-local multicast). Select the API version used in the **API version** field. Defaults to **v1.3**. **DNS-SD** - Use this if the NMOS registry service is advertised by the current DNS server (network service discovery is via DNS). Select the API version used in the **API version** field. Defaults to **v1.3**. **Manual** - Use **Manual** if you already know the NMOS registry service. **Manual address**: In the field, enter the NMOS registry server address. **Manual registration port**: Enter the port number to use for the NMOS registration API. This will be used to register the device to a registry server. **Manual query port**: Port to use for the NMOS query API to receive updates from a registry server and discover new devices.
API version	Select **v1.2** or **v1.3**.

Enable NMOS

In the default setting, NMOS is disabled. To enable NMOS:

Step 1. When logged in as an administrator, from the left navigation menu, select **Device**.

Step 2. Click the **NMOS** tab.

Step 3. From the **NMOS** section on the right, click the **Enable NMOS** check-box to enable NMOS registration.

Step 4. From the **NMOS node** and **NMOS registry server** sections to the right, make your selections.

Result of this task: The default node used is port 5051. The registry server discovery uses **Automatic DNS-SD** or **MDNS**.

Other

From here, you can see the temperature readings, enable or disable the functioning of the buttons on the device, and also trigger the LEDs to flash to make it easy for you to spot where the device is located.

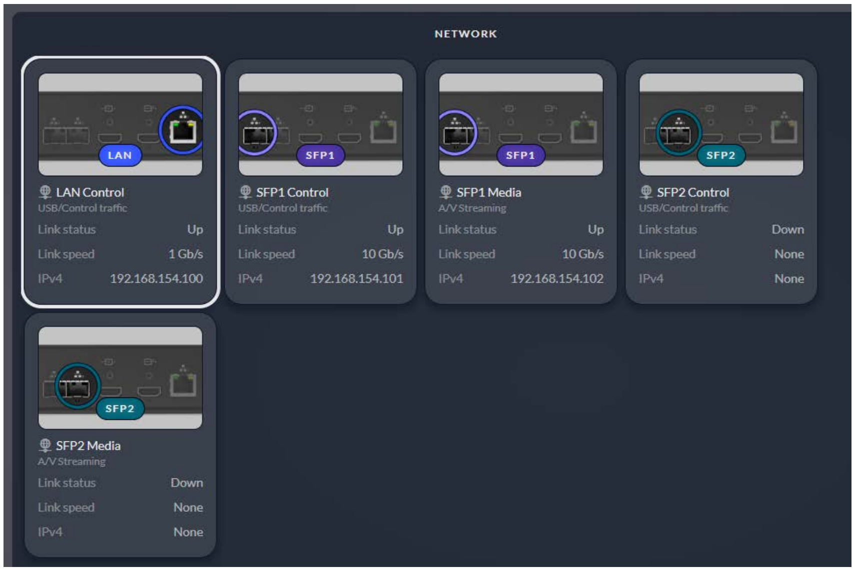
Setting	Description
Other	
Temperature	Displays the temperature of the **CPU**, **SFP1**, and **SFP2**. Displays in **Celsius** or **Fahrenheit** depending on the **Temperature unit** selected in the **PREFERENCES** screen. Temperatures over the threshold will appear in bright red. The safe operating threshold temperature is 80 degrees Celsius for the CPU and 85 degrees Celsius for commercial SFP modules. (Industrial grade SFP modules could have a higher threshold.) SFP ports with no SFP module attached will display **N/A**.

Physical buttons	This toggle button is enabled by default. To make the physical buttons on the front of the Avio 2 device non-operational, toggle this button to the disabled position.
Locate device	By default, this is disabled. When you enable this switch, the LEDs on the front and back of the device flash for five (5) minutes making it easy for you to locate the device. **Front LEDs**: Tx, Status, and Rx **Back LEDs**: HDMI in and HDMI out If you do not disable the option after enabling, it goes back to the default position of being disabled after five minutes.

Network settings

From here you can manage the network settings for your Avio 2 device.

NOTE The Network settings options are similar for the receiver and the transmitter.



LAN Control
USB/Control traffic
Link status Up
Link speed 1 Gb/s
IPv4 192.168.154.100

SFP1 Control
USB/Control traffic
Link status Up
Link speed 10 Gb/s
IPv4 192.168.154.101

SFP1 Media
A/V Streaming
Link status Up
Link speed 10 Gb/s
IPv4 192.168.154.102

SFP2 Control
USB/Control traffic
Link status Down
Link speed None
IPv4 None

SFP2 Media
A/V Streaming
Link status Down
Link speed None
IPv4 None

In the **Network** page, there is a tile for each network interface.

- **LAN Control** - This is the LAN that receives the control commands for Avio 2 settings. This is typically set to DHCP in most cases. If you set this to static, you'll need to specify the corresponding IP address and network information.
- **SFP1 Control** - This is the Network interface name for USB and control via SFP Media 1 physical port.
- **SFP1 Media** - This is the Network interface name for A/V streams via SFP Media 1 physical port. This is the LAN that receives video/audio content.
- **SFP2 Control** - This is the Network interface name for USB and control via SFP Media 2 physical port.
- **SFP2 Media** - This is the Network interface name for A/V streams via SFP Media 2 physical port. This is the LAN that receives video/audio content.

Each tile shows the basic details such as its intended usage (USB/Control traffic or A/V Streaming), link status, link speed, and IP addressing (IPv4).

The image of the box at the top of each tile shows on which physical network connector the interface is located by highlighting it with a circle. On the tiles, the interfaces located on the same physical network connector have the same badge (SFP 1 or SFP 2) color. The color of the circle highlighting the matching physical port on the box is also in the same color.

NOTE When you change any network settings for SFP1 Media or SFP2 Media, you need to reboot the device for the changes to take effect.

Global settings

The **Global settings** fields are common for all the five network interfaces.

Setting	Description
Global settings	
SFP Module Speed	Displays the link speed for the SFP module. The speed at boot up, according to the cable connected in the first SFP connector.
Device Hostname	You can edit the device's hostname from here. The Linux hostname limitations are: • Each element of the hostname must be from 1 to 63 characters long. • The entire hostname, including the periods, can be a maximum of 253 characters. • Valid characters for hostnames are ASCII(7) letters from a to z, the digits from 0 to 9, and the hyphen (-). • A hostname must not start with a hyphen. **NOTE**: Changing the device's hostname has an impact on HTTPS or TLS certificate validation as the device certificate has to match the hostname. So, when you deploy your own certificates, make sure the hostname matches the one mentioned in the certificate. If you change the hostname alone without deploying the corresponding certificate, HTTPS or TLS validation of the device certificate will not take place. In this case, a warning will display on the **Device** page.

Network connector	The device's configured network control connector. Select **LAN Control**, **SFP1**, or **SFP 2**. This sets which network port the following network traffic would go through: • Remote Web user interface • NMOS discovery traffic • MDNS and LLMNR traffic • NTP related traffic **NOTE**: Changing the network interface will make the Web UI change its required IP address.
IGMP control	Rx - Select **None**, **IGMPv2**, or **IGMPv3**. Tx - Select **None** or **IGMPv2**.
MDNS	Enable **MDNS** if you would like your Avio 2 device to use this discovery method to announce itself on the network so it can be found by other devices or applications. Enable MDNS to broadcast the Avio 2 internal NMOS registry on the network under the multicast DNS protocol. This resolves hostnames to IP addresses within networks that do not include a domain name server. Multicast DNS publication only works with devices on the same subnet.
LLMNR	Enable LLMNR (Link-Local Multicast Named Resolution) if you would like your Avio 2 device to use this discovery method to announce itself on the network so it can be found by other devices or applications. Enable Link-Local Multicast Name Resolution to allow an IPv4 host to perform name resolution for hosts on the same local link.

When you click on a network interface tile, detailed information related to the network is shown on the right panel under three tabs.

- **Info tab** - This tab holds the current status of the interface and all settings currently in effect for the selected network interface.

- **Connector tab** - This tab holds information specific to the physical connector (and shared between interfaces on this connector).
- **IP tab** - This tab holds all the IP settings editable by an administrator. **NOTE**: You need to be logged in as an administrator to be able to even see this tab.

The fields in these tabs are the same for **LAN Control**, **SFP1 Control**, **SFP1 Media**, **SFP2 Control**, and **SFP2 Media**.

Setting	Description
Info tab	
Physical address	The MAC address. This is unique and cannot be changed.
MTU	The Maximum transmission unit defaults to **1500**.
IPv4	Displays the IPv4 address assigned for the selected network interface.
Net mask	The IPv4 network mask.
DNS servers	The IPv4 DNS servers.
Connector tab	
Link status	Displays the status of the link.
Link speed	Displays the negotiated link speed.
IP tab	
Search domains	Enter a list of domains here, separated by space, to be used for DNS lookups and resolution.

IPv4	Following are the IPv4 options: • **DHCP** - When you select an address manually, by disabling the DHCP switch, the current values (typically assigned by the DHCP) are wiped out in the fields. You will however be able to see the current IP on the device tile. • **IP address** - This is mandatory when configuring a static IP address. • **Netmask** - This is mandatory when configuring a static IP address. • **Gateway** - The gateway address. • **DNS servers** - Enter a list of IPv4 addresses (separated by space) for the DNS servers.

Users settings

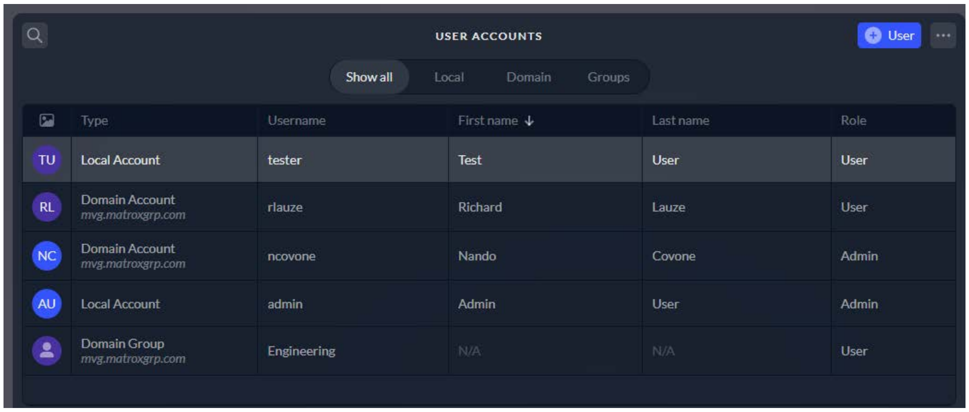
The **Users** menu option is visible only to admin users.

In Receiver mode, as an admin user you can see and edit all the settings in the UI and connect to authorized transmitters. As a regular (non-admin) user in Receiver mode, you will only be able to see the authorized transmitters and connect to them, as well as view some information.

Administrator	User
• Create other admin and regular users; import users list using JSON file • Add, delete, and change passwords for all users • Authorize transmitters • Connect to authorized transmitters • Change the device name • Update device firmware • Reboot the device • Configure network settings • Configure device settings • Configure date and time settings (NTP and PTP) • Modify EDID • Create shortcuts for transmitters and OSD • Add and delete certificates and licenses • Download and disable certificates • Modify NMOS settings • Modify encryption and compression settings • Allow or disallow USB groups • Set up redundancy • Delete device logs • Download updates and device logs • Erase device and processing data	• Connect to authorized transmitters • View device info • View AV processing information • Change temperature unit and keyboard preferences • Add a folder • Change the audio levels

In Transmitter mode, you will be able to sign in only if you are an admin user. As an admin user you can see and edit all the settings in the UI. In addition to all the tasks mentioned above (for the Administrator in Receiver mode), the admin user in Transmitter mode will be able to set the access control (allow multiple receivers to connect to a transmitter).

NOTE The **Users** settings options are similar for the receiver and the transmitter. What you see in the UI will depend on whether you are logged in as an admin or regular user.



	Type	Username	First name ↓	Last name	Role
TU	Local Account	tester	Test	User	User
RL	Domain Account mvg.matroxgrp.com	rlauze	Richard	Lauze	User
NC	Domain Account mvg.matroxgrp.com	ncovone	Nando	Covone	Admin
AU	Local Account	admin	Admin	User	Admin
	Domain Group mvg.matroxgrp.com	Engineering	N/A	N/A	User

Admin user

When a device is accessed for the first time, or after a reset to default, no user account exists on the device. The first thing you have to do is create a new user in the sign-up screen that displays in the UI. The first user that your create is the first admin account. This first admin account must be a local user account as local user passwords are validated on-device. Active Directory / LDAP user account is not allowed for the first admin account as Active Directory / LDAP user passwords need to be validated with the AD / LDAP server. For adding subsequent admin users, Active Directory / LDAP user account is allowed.

Create the first admin user account

To create the first admin local user account:

Step 1. In the **WELCOME** screen that displays, click the **Sign up** button.

Step 2. Enter the first name in the **First name** and the last name in the **Last name** fields. The first and last names must be between 2 and 50 characters with no white space in the first and last character.

Step 3. Enter the full user name in the **Username** field. The username must be between 2 and 50 characters with no white spaces.

Step 4. In the **Password** field, enter between 10 and 64 characters with at least one in upper case, one in lower case, one number, and one special character (!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~).

Step 5. Once the password format validation is done, the **Sign up** button displays at the bottom. Click the **Sign up** button.

Step 6. Click **Accept** in the software license agreement screen that displays.

Result of this task: The first admin account is created on the device.

User accounts

There are two types of user accounts in Avio 2.

- **Local user account** - Local user accounts are accounts created on the device and their passwords are validated on the device. A local user account's password can be changed by any administrator.
- **Domain user account** - Domain user accounts are defined on an Active Directory domain and those existing accounts are added to the list of valid users of the Avio 2 device. A domain user account could be an *Active Directory domain - LDAP account* or an *Active Directory domain - LDAP group account* which represents a group of users on an Active Directory domain. When adding a domain user account to the list of users on an Avio2 device, the device looks up the user account with the AD server to ensure the account exists. No password is provided to the device when adding the domain user account to the device. An AD / LDAP account password can't be changed through the Avio 2 device. This has to be done through the relevant AD server password change procedures.

Access or edit user accounts

To view or edit the user accounts, you need to be logged-in as an admin user.

Step 1. Make sure you are logged-in as an admin user.

Step 2. From the left navigation menu, select **Users**.

Result of this task: The list of **USER ACCOUNTS** displays.

User accounts list

From the left menu, select the **Users** option. The list of **USER ACCOUNTS** displays the following information:

Setting	Description
USER ACCOUNTS	
Type	The type of user account - **Local Account**, **Domain Account**, or **Domain Group**.
Username	The full user name.
First name	The first name of the user.
Last name	The last name of the user.

Role	Options are **Admin** and **User**. An admin user can't change their own role.
Filters	
Show all	Displays all the user accounts. **NOTE**: By default all the user accounts are displayed. For the **Filters** option to display, there should be at least a mix of two users from two of the three following user filter options: Local, Domain, and Groups.
Local	Displays only the local user accounts.
Domain	Displays only the domain user accounts.
Groups	Displays only the domain group accounts.

Sort the user account list

This **USER ACCOUNTS** list can be sorted. By default, the list displays in the alphabetical order of the Username. You can sort it by column heading by hovering over the column heading until you see an arrow icon and then clicking on it. The user accounts can be sorted in ascending or descending alphabetical order on the column values.

User properties

When you click on a user account from the **USER ACCOUNTS** list, the properties display in the right panel as well for the selected user account.

- First name
- Last name
- Username
- Role

From here, you can click the **Change** button to change the password for the user account.

Create a new local user account (admin or user)

To create a new local user account:

Step 1. Make sure you are logged-in as an admin user.

Step 2. From the left navigation menu, select **Users**. The list of **USER ACCOUNTS** displays.

Step 3. Click the **+User** button on the top of the list.

Step 4. Select the **Local account** option.

Step 5. Enter the first name in the **First name** and the last name in the **Last name** fields. The first and last names must be between 2 and 50 characters with no white space in the first and last character.

Step 6. Enter the full user name in the **Username** field. The username must be between 2 and 50 characters with no white spaces.

Step 7. In the **Role** field, select **User** or **Admin**. **NOTE**: The color of the user icon displays in blue for an Admin user and in purple for a regular user.

Step 8. In the **Password** field, enter between 10 and 64 characters with at least one in upper case, one in lower case, one number, and one special character (!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~).

Step 9. Click OK.

Result of this task: The local user account is created on the device.

When done, remember: You can delete the user account by clicking the more (**...**) button on top of the **USER ACCOUNTS** list and selecting **Delete**.

NOTES

- There has to be at least one admin account. The last user account in the list with the **Admin** role cannot be deleted. The only way you can remove all the user accounts is by performing a configuration reset.
- An account with the **User** role cannot log into a transmitter.
- User names are case insensitive so you will not be able to add a new user with just the case being different from an existing user account. For example, if you have “JaneSmith” as an existing username, you will not be able to create a new user account with “janesmith” as the user name.
- A log-in is valid for 72 hours. When you refresh the web UI (**F5**) after this time, you will be taken to the log-in screen. To have a secure connection with the AD / LDAP server, you need to add the Certificate Authority (CA) used to sign the AD / LDAP server.

Create a new domain user account (admin or user)

To create a new domain user account:

Step 1. Make sure you are logged-in as an admin user (domain account with valid AD credentials, or local account).

Step 2. From the left navigation menu, select **Users**. The list of **USER ACCOUNTS** displays.

Step 3. Click the **+User** button on the top of the list.

Step 4. Select the **Domain account** or the **Domain group** option.

Step 5. If you logged in with your local account, the **DOMAIN CREDENTIALS** screen displays. (**NOTE**: This screen will not display if you are logged in already with your domain account.) Enter your domain account credentials in the **Account name**, **Domain name**, and **Password** fields. Your user account is verified with the AD server to ensure the account exists.

Step 6. In the **Role** field, select **User** or **Admin**. **Note**: The color of the user icon displays in blue for an Admin user and in purple for a regular user.

Step 7. Click OK.

Result of this task: The domain user account is created. No password is provided to the device. The AD user, or any AD user member of the domain group will be allowed to log into the device.

When done, remember: You can delete the user account by clicking the more (**...**) button on top of the **USER ACCOUNTS** list and selecting **Delete**.

Log into a local user account

To log into a local user account:

Step 1. Enter your user name in the **User name** field.

Step 2. Enter your password in the **Password** field. Your password is between 10 and 64 characters with at least one in upper case, one in lower case, one number, and one special character (!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~).

Step 3. Click **Log in**.

Result of this task: You are logged into the device.

NOTES

- Your log-in via the web browser is valid for 72 hours whereas your OSD log-in never expires. After 72 hours of being logged into the user interface through the web browser, you will be taken to the login screen where you will have to log in again.
- When you refresh the web UI (**F5**) after this time, you will be redirected to the log-in screen.
- A user account can be logged into only one session for a device. If you log into multiple web browser tabs or the OSD, you will be able to apply changes only in your latest log-in session. You will be logged out of the other log-in sessions.
- An account with the **User** role cannot log into a transmitter.
- To allow a secure connection with the AD / LDAP server, you need to add the Certificate Authority (CA) used to sign the AD / LDAP server.

CHAPTER 5

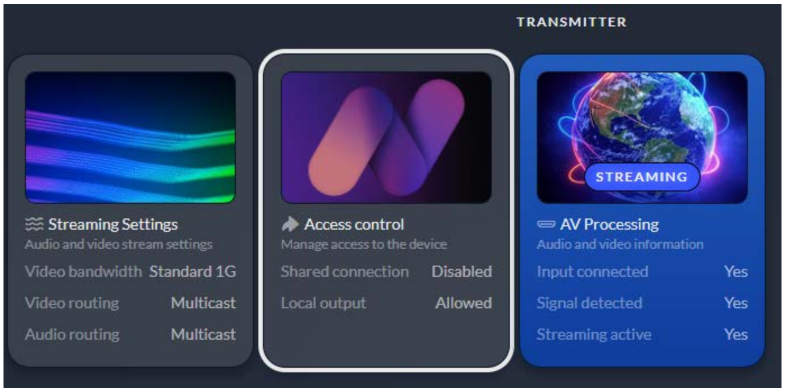
Matrox Avio 2 Transmitter settings

This chapter includes the following topics:

- *Transmitter settings*
- *Device settings*
- *Network settings*
- *Users settings*

Transmitter settings

You can manage the streaming and the access settings to the device from here. You can also view the A/V processing details from here.



TRANSMITTER

Streaming Settings
Audio and video stream settings

Video bandwidth	Standard 1G
Video routing	Multicast
Audio routing	Multicast

Access control
Manage access to the device

Shared connection	Disabled
Local output	Allowed

STREAMING

AV Processing
Audio and video information

Input connected	Yes
Signal detected	Yes
Streaming active	Yes

Streaming

Using the **Streaming** tile, you can set the audio and video stream settings. The following information is displayed on the tile:

- Video bandwidth
- Video routing
- Audio routing

Avio 2 transmitters can send the video content over the network either uncompressed or compressed. For sending compressed video content, JPEG XS and ProAV codecs are supported.

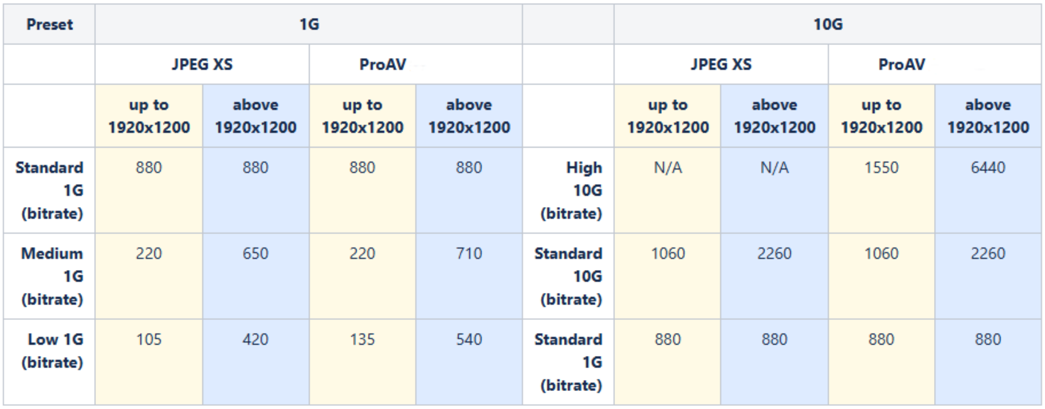
ProAV comes built-in with Avio 2 and does not need a license file. JPEG XS codec requires a license to be purchased from Matrox and deployed on the device.

Setting	Description
Streaming settings	
Video compression	Toggle button to enable or disable video compression. By default, video compression is enabled.
Video bitrate level	For each codec (JPEG XS and ProAV), three target bit rate presets of **Standard 1G**, **Standard 10G**, and **High 10G** are available that can be used to control the codec's operation. The default is **Standard 10G**. For more information see "*Presets bit rates*" on page 76. When none of these presets are suitable for your operation, you can set an arbitrary target bit rate using the **Custom** option. You need to provide the target bit rate for **Up to 1920x1200** and **Above 1920x1200** using the figures in the Presets bit rate table for guidance.
Audio source	Avio 2 supports a single audio stream from the Tx. **NOTE**: You need to be an administrator to set which audio input to use as the source. **Analog (line in)** - Select when analog audio in is used. **HDMI audio** - Select when HDMI in audio is to be used.
Redundancy	Click the toggle button to enable redundancy. **NOTE**: In the initial release (v1.00), only audio and video are supported. There is no redundancy support for USB streaming.
Video stream routing	
Routing scheme	Select **Unicast** or **Multicast**.

Destination IP address	Enter the Destination IP address for Multicast video stream routing.
Destination port	Enter the Destination port number for Multicast video stream routing.
Audio stream routing	
Routing scheme	Select **Unicast** or **Multicast**.
Destination IP address	Enter the Destination IP address for Multicast audio stream routing.
Destination port	Enter the Destination port number for Multicast audio stream routing.

Presets bit rates

The current preset's actual bit rates depend on the codec being used and the speed rating of the SFP module (1 Gbps or 10 Gbps) as detailed in the table below.



Preset	1G					10G			
	JPEG XS		ProAV			JPEG XS		ProAV	
	up to 1920x1200	above 1920x1200	up to 1920x1200	above 1920x1200		up to 1920x1200	above 1920x1200	up to 1920x1200	above 1920x1200
Standard 1G (bitrate)	880	880	880	880	High 10G (bitrate)	N/A	N/A	1550	6440
Medium 1G (bitrate)	220	650	220	710	Standard 10G (bitrate)	1060	2260	1060	2260
Low 1G (bitrate)	105	420	135	540	Standard 1G (bitrate)	880	880	880	880

NOTE The bit rate specified is the expected bit rate for the highest resolution for the specific criteria. For example, a 1G SFP module using the JPEG XS codec with the Standard 1G preset is expected to use 880 Mbps when the input signal is 1920x1200 @ 60 Hz or up to 4K @ 60 Hz.

Access control

An administrator can set a transmitter to share its video, audio, and USB connection with multiple guest receivers while a main receiver is already connected to the transmitter. The admin can also allow the guest receiver to view and control the source locally using the video passthrough and the transmitter’s local USB connectors.

Once set, a receiver and/or a local user can connect as a guest to a transmitter.

The **Access control** tile displays the source sharing settings that have been selected.

- **Shared connection** - Displays the status of the shared connection over the network - whether **Disabled** or **Allowed**.
- **Local output** - Displays **Disabled** or **Allowed**.

Setting	Description
Source sharing	
Shared connection	Set the source sharing options for a guest receiver here. **Audio, video, and USB** - Guests can receive the audio and video signal, and also control using USB devices (one-to-many connection). **Audio, video** - Guests can receive the audio and video signal but will not be able to control using USB devices (one-to-many connection). **Disabled** - Guests will not be able to connect to the transmitter. The default is **Disabled** (one-to-one connection only).
Local output	Set the source sharing options for guests on the local output of the transmitter. **Audio, video, and USB** - Guests can receive the audio and video signal, and also control using USB devices (one-to-many connection). **Audio, video** - Guests can receive the audio and video signal but will not be able to control using USB devices (one-to-many connection). **Disabled** - Guests will not be able to connect to the transmitter. The default is **Disabled** (one-to-one connection only).

NOTES

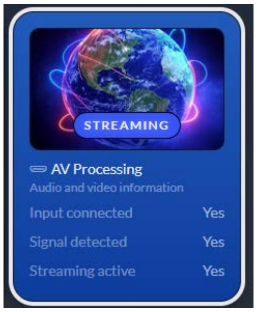
- The first receiver to connect to the transmitter will take ownership of the connection.
- When a receiver is already connected, and guests are allowed, the next receiver to connect becomes a guest of the connection.

- If a receiver with ownership of a connection disconnects when guests are still connected, the guests will not be able to take the ownership of the connection. The next receiver that connects will get the ownership of the connection.
- The options can be changed live while guests are still connected, but only if you change to a lower permission level setting. For example, you can change from **Audio, video, and USB** to **Audio, video** or **Disabled**. Or, from **Audio, video** to **Disabled**. Connected guests will automatically disconnect and reconnect to the transmitter using the new setting. If set to **Disabled**, the guest receiver will disconnect and display that guest connection is no longer allowed.
- To apply a setting with a higher permission level than the current one, the guest user will have to first disconnect then reconnect to the transmitter.

AV processing

Avio 2 transmitters have an HDMI input and an analog audio input. When an input signal is detected, the details are displayed.

It also shows the current status of the AV processing status of the transmitter.



AV Processing
Audio and video information

Input connected Yes
Signal detected Yes
Streaming active Yes

When the transmitter does not have a physical cable connected to its HDMI input, the AV Processing tile displays in a disabled state with the message **NO CABLE DETECTED**.

The tile will also display the following information.

Field	Description
AV Processing	
Input connected	Displays **Yes** when a physical cable is connected to the transmitter's HDMI input, otherwise **No**.
Signal detected	Displays **Yes** when a signal is detected, otherwise **No**.
Streaming active	Displays **Yes** when streaming, otherwise **No**.

When a cable is connected to the transmitter, the tile will display **CABLE CONNECTED** momentarily, and then display whether it is in an idle or non-streaming state. When you click on the tile, the input signal details of the transmitter will show in the right panel.

Field	Description
Input details	
Video input	Resolution and frame rate of the input signal/stream.
Bit depth	Displays the bit depth of the stream.
HDMI audio input	Displays the HDMI audio input details.
HDMI audio channels	Displays details of the HDMI audio channels being used.
Analog audio input	Displays the analog audio input details.
Analog audio channels	Displays details of the analog audio channels being used. Describes how the analog signal is sampled and encoded internally.

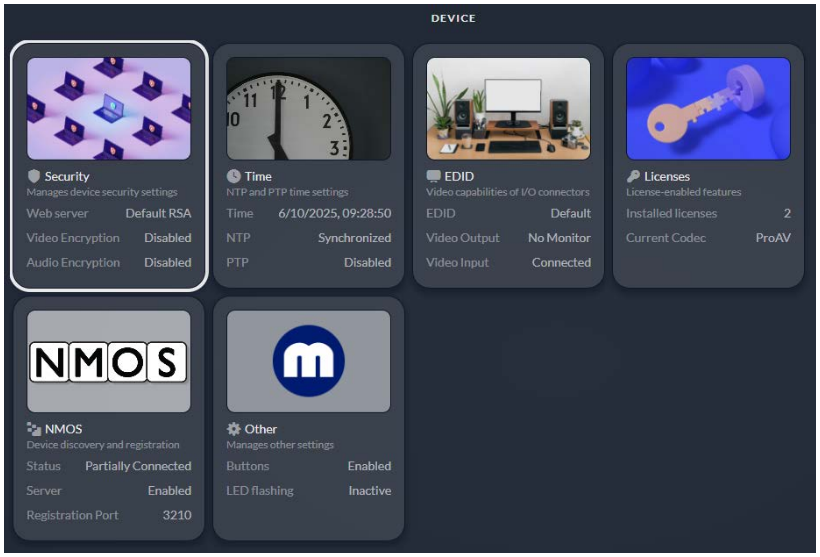
When the transmitter starts streaming, the tile will display **STREAMING**. When you click on the tile, the input signal information as well as the streaming details for both audio and video appear in the right panel. You can copy the audio and video SDP URLs to the clipboard.

Field	Description
Video stream	
Stream label	The stream label displays the device name appended with Video Sender followed by a number.
Resolution	Displays the resolution and frame rate of the video stream.
Bit depth	Displays the bit depth of the stream.
Scaling	This displays any scaling performed on the Rx on the incoming stream prior to displaying. Otherwise, displays **No scaling**.

Compression type	Displays the compression type used - **Uncompressed**, **JPEG XS** or **PRO-AV**.
Bandwidth	Displays the current bandwidth being used.
Encryption	Displays **Active** when the video stream is encrypted, otherwise **Inactive**.
SDP file URL	Click the **Copy to clipboard** button to copy the SDP file URL to the clipboard. **NOTE**: The SDP file will be available only if NMOS is enabled. The SDP URLs are HTTP (not HTTPS), as is customary for SDP files.
Audio stream	
Stream label	The stream label displays the device name appended with Audio Sender followed by a number.
Audio format	Displays the format of the audio stream.
Source	Displays HDMI audio or Analog audio.
Encryption	Displays **Active** when the audio stream is encrypted, otherwise **Inactive**.
SDP file URL	Click the **Copy to clipboard** button to copy the SDP file URL to the clipboard. **NOTE**: The SDP file will be available only if NMOS is enabled. The SDP URLs are HTTP (not HTTPS), as is customary for SDP files.

Device settings

See "*Device settings*" on page *45*.



DEVICE

Security
Manages device security settings

Web server	Default RSA
Video Encryption	Disabled
Audio Encryption	Disabled

Time
NTP and PTP time settings

Time	6/10/2025, 09:28:50
NTP	Synchronized
PTP	Disabled

EDID
Video capabilities of I/O connectors

EDID	Default
Video Output	No Monitor
Video Input	Connected

Licenses
License-enabled features

Installed licenses	2
Current Codec	ProAV

NMOS
Device discovery and registration

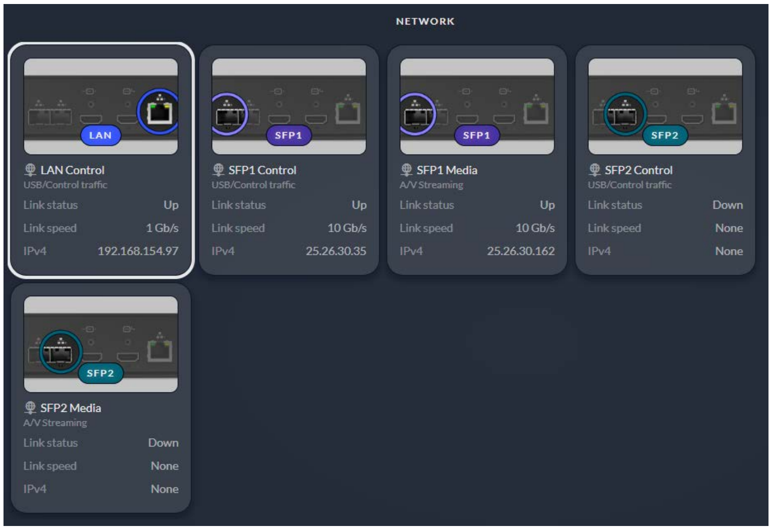
Status	Partially Connected
Server	Enabled
Registration Port	3210

Other
Manages other settings

Buttons	Enabled
LED flashing	Inactive

Network settings

See "*Network settings*" on page *62*.



NETWORK

LAN Control
USB/Control traffic
Link status Up
Link speed 1 Gb/s
IPv4 192.168.154.97

SFP1 Control
USB/Control traffic
Link status Up
Link speed 10 Gb/s
IPv4 25.26.30.35

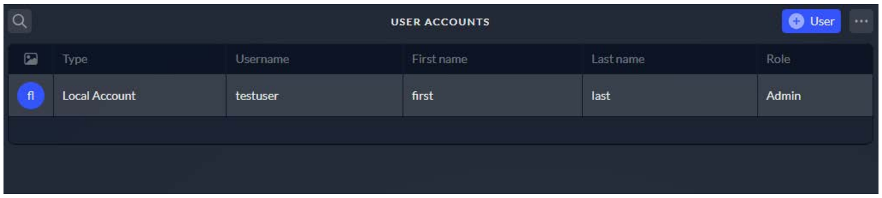
SFP1 Media
A/V Streaming
Link status Up
Link speed 10 Gb/s
IPv4 25.26.30.162

SFP2 Control
USB/Control traffic
Link status Down
Link speed None
IPv4 None

SFP2 Media
A/V Streaming
Link status Down
Link speed None
IPv4 None

Users settings

See "*Users settings*" on page *67*.



	Type	Username	First name	Last name	Role
fl	Local Account	testuser	first	last	Admin

CHAPTER 6

Hardware specifications

This chapter includes the following topics:

Matrox Avio 2 Technical specifications

In this section, you will find the hardware and software specifications for the Matrox Avio 2 device.

	Avio N2150
Part number	AV2-N2150 AV2-N2150Y (TAA compliant)
Form factor	Appliance (1U, 1/2R)
Connectivity	
Video input connector	Tx - HDMI Rx - Not applicable
Video output connector	Tx - HDMI zero-latency passthrough Rx - HDMI
Audio input / output	Tx - Line in 3.5 mm, line out 3.5 mm[1] Rx - Line out 3.5 mm, mic in 3.5 mm[1], headphone out 3.5mm
Network connectors	• 1x RJ45 LAN control port (1GbE) • 2x SFP cages for media and/or control (1GbE or 10GbE
USB port	Tx - 2x USB2.0 Type A for local keyboard and mouse Tx - 1x USB2.0 Type B for host system connection Rx - 4x USB2.0 Type A
5-pin Phoenix connector	RS232[1]
Performance	
Max video resolution	4096x2160@60Hz 4:4:4 3840x2160@60Hz 4:4:4 All standard desktop GPU resolutions are supported.

Color space and bit depth	RGB 4:4:4 8-bit, YUV 4:4:4, YUV 4:2:2, YUV 4:2:0[2] 8-bit, 10-bit SDR, HDR
USB support	High Speed USB 2.0: Keyboard, mouse, touchscreens, pen tablets, joysticks, and other USB HID devices, smart card/CAC readers, USB 2.0 (full speed) speakers / sound bars, USB headsets
Audio support	Digital embedded audio (HDMI) Stereo analog audio – 2 channels
Network speed	1GbE or 10GbE
Maximum distance (point-to-point)	**Copper SFP**: 1GbE RJ45 Cat5e, Cat6—100 m (328 ft) 10GbE Cat6a—100 m (328 ft) **Fiber SFP**: • OM1 (62.5/125µm) multi-mode - 275 m (902 ft) • OM2, OM3, OM4 (50/125µm) multi-mode – 500m (1804 ft) • OS1, OS2 (9/125µm) single-mode - 10 km (6.20 mi) **Fiber SFP+**: • OM1 (62.5/125µm) multi-mode - 33 m (108 ft) • OM2m, OM3, OM4 multi-mode – 300m (984 ft.) • OS1, OS2 (9/125µm) single-mode - 10 km (6.20 mi)
On-screen-display (OSD)	Available in receiver mode.
Encoding formats	
Video	• Matrox Pro AV • ISO/IEC JPEG XS (optional upgrade) Designed and optimized for 1 Gbps. Can support lower video bandwidth (<100 Mbps) or scale up for maximum quality (≥2Gbps).[3]
Audio	Uncompressed PCM (~1 Mbps/c)

Network	
Network standard	**Control Port**: 1000 Base-T Ethernet Auto-detect Full / Half duplex **Media port**: 1 GbE, 10 GbE
Supported protocols	• IPMX TR10-XXX • SMPTE ST 2110 (-10, -20, -21, -22, -30, -31, and -40) • SMPTE ST 2059-2, 2059-1 • SMPTE ST 2022-7
Routing scheme	• Multicast • Unicast
IP addressing	• IPv4 • IPv6[1] • DHCP (default) and Static IP
Link redundancy	SMPTE 2022-7
Link aggregation	Available for uncompressed 4Kp60 (Link redundancy is disabled in this mode)
Command and control	HTTPS over TCP
Discovery, registration, and control	• NMOS discovery and control according to standards IS-04 and IS-05 (optional) • mDNS discovery
Physical	
Physical dimensions	7.3” (W) x 7.126” (L) x 1.545” (H)
Unit weight	820 grams
Power supply unit	External 40W PSU with lockable PSU connector (optional, sold separately)
PoE+	PoE+ IEEE 802.3at
Cooling	Fanless cooling
Security	
HTTPS Digital Certificates	Yes

AES encryption	AES-128 for audio, video, and USB
User management	Local and Microsoft® Active Directory® support for groups and domain
User roles	Admin, User
Accessories (sold separately)	
Rack-mount kit	Part #: RMK-19TR-A
Mounting bracket	Part #: RMK-6BRKT-A
Power supply unit	Part #: EPS40WKIT-NA, EPS40WKIT-EU, EPS40WKIT-UK, EPS40WKIT-AU, EPS40W-10PK[4]
NRG redundant power supply unit	Part #: NRG-5-1DB or NRG-5-2DB
KMLync switch	Part #: KMLYNC-4Y-NA, KMLYNC-4Y-EU, KMLYNC-4Y-UK, KMLYNC-4Y-AU,
Multi-Mode Fiber Optic Transceiver (XTO3-SFPMM)	1x 1.25Gbps SFP multi-mode transceiver
Single-Mode Fiber Optic Transceiver (XTO3-SFPSM)	1x 1.25 Gbps SFP single-mode transceiver
RJ45 Copper Transceiver (SFP-RJ45H-1G)	1x 1 Gbps RJ45 SFP transceiver
Software (optional)	
JPEG XS codec license	Part #: AV2-JXS-UPG
Environmental conditions	
Operating conditions	**Temperature**: 0 to 45 degrees Celsius **Altitude**: 650 hPa (3,580 m) to 1,013 hPa (0 m) **Humidity**: 20% to 80% non-condensing

Storage conditions	**Temperature**: -40 to 70 degrees Celsius **Altitude**: 192 hPa (12,000 m) to 1,020 hPa (-50 m) **Humidity**: 5% to 95% non-condensing
General	
EMC/EMI device class	Class A
EMC/EMI compliance	• CE (EU) • FCC (USA) • ICES-003 (Canada) • KC (Korea) • RCM (Australia/NZ)
Environmental compliance	• China RoHS • EU RoHS • REACH
Warranty	Three year limited warranty with free online or telephone support. Extended warranty available. For more information, contact Matrox Video.

1. Available in a future software release.
2. YUV 4:2:0 is input-only, then upscaled to YUV 4:2:2.
3. Bit rates will vary according to the resolution, frame rate, and codec option.
4. Part # EPS40W-10PK does not include IEC-C14 power cord. These cables must be sourced locally.

Notes and limitations

The following are some notes and known limitations in Avio 2 release 1.00.

- IPv6 is not supported.
- On Windows systems, the Avio 2 default EDID always streams in 4K, even if the desktop resolution is set to a different resolution.
- On macOS hosts, temporal dithering degrades visual quality when using the ProAV codec. Disable temporal dithering for best results.
- Changing the following options during an active connection is not supported: PTP, network routing scheme, audio configuration (HDMI to analog and vice versa), and video encoding options.
- The SDP file is not accessible if NMOS is disabled on the transmitter, even though the file is available.

CHAPTER 7

Customer support

This chapter includes the following topics:

Customer support

In this section, you will find customer support information for your Matrox Avio 2 device.

Matrox Video web

Our web site has product literature, press releases, technical material, a sales office list, trade show information, and other relevant material. Visit the Matrox Video web site at *video.matrox.com*.

Technical support

Matrox Video values your business and offers professional support for your Matrox Video product.

If your product was purchased through a Matrox Video dealer, contact your dealer for product support. This is the quickest and most effective method of technical assistance. Your dealer is familiar with your complete system.

If your product was purchased through Matrox Video, contact your Matrox Video representative or visit our technical support Web site at video.matrox.com/en/support.

To serve you better, please provide a complete description of the problem, and include:

- Matrox product serial number, model number, revision number, and firmware number.
- Source specifications
- Specific web UI or OSD options and features used.

Register your Matrox Video product

Please register online (*video.matrox.com/en/apps/registration*) to be eligible for customer support, new product announcements, and information on special offers and upcoming events.

Disclaimers

(English) Disclaimer

THE INFORMATION IN THIS GUIDE IS SUBJECT TO CHANGE AT ANY TIME AND WITHOUT NOTICE.

Matrox Graphics Inc. reserves the right to make changes in specifications at any time and without notice. The information provided by this document is believed to be accurate and reliable at the time it is written. However, no responsibility is assumed by Matrox Graphics Inc. for its use, for its reproduction and/or distribution, in whole or in part; nor for any infringements of patents or other rights of third parties resulting from its use.

(Français) Responsabilité

LES INFORMATIONS CONTENUES DANS CE MANUEL PEUVENT ÊTRE MODIFIÉES EN TOUT TEMPS ET CE SANS PRÉAVIS.

Les Graphiques Matrox Inc. se réserve le droit de modifier les spécifications en tout temps et ce sans préavis quelconque. Les informations contenues dans ce manuel sont reconnues comme étant précises et fiables à la date de rédaction. Cependant, Matrox Graphics Inc. n’assume aucune responsabilité concernant leur utilisation, leur reproduction et/ou distribution, en tout ou en partie, ni leur contrefaçon de brevets ou de tout autre droit appartenant à des tiers résultant de leur utilisation. Aucune licence n’est accordée sur aucun brevet ou droit d’exploiter un brevet de Matrox Graphics Inc.

(Deutsch) Haftungsablehnungserklärung

DIE IN DIESEM HANDBUCH ENTHALTENEN ANGABEN UND DATEN KÖNNEN OHNE VORHERIGE ANKÜNDIGUNG GEÄNDERT WERDEN.

Die Matrox Graphics Inc. behält sich das Recht vor, jederzeit und ohne Ankündigung technische Daten zu ändern. Zum Zeitpunkt der Erstellung dieses Handbuchs sind die Inhalte korrekt und verlässlich. Weiterhin übernimmt Matrox Graphics Inc. keinerlei Verantwortung für die Benutzung dieses Handbuchs, die Vervielfältigung und/oder Verteilung im Ganzen oder zum Teil; weder für Verstöße gegen Patentrechte noch für andere Rechte Dritter, die aus seinem Gebrauch resultieren mögen. Es werden keinerlei Lizenzrechte gewährt für sämtliche Patente oder Patentrechte der Matrox Graphics Inc.

(Italiano) Discrezionalità

LE INFORMAZIONI CONTENUTE NEL PRESENTE DOCUMENTO SONO SOGGETTE A MODIFICHE IN QUALUNQUE MOMENTO E SENZA PREAVVISO.

Matrox Graphics Inc. si riserva il diritto di apportare variazioni di qualunque tipo alle specifiche tecniche in qualunque momento e senza alcun preavviso. Le informazioni contenute in questa documentazione sono ritenute corrette e attendibili al momento della pubblicazione. In ogni caso, non è imputabile a Matrox Graphics Inc. nessuna responsabilità per il loro utilizzo, per la loro distribuzione e/o riproduzione completa o in parte, come nessuna violazione a brevetti o diritti di altri produttori derivante dal loro utilizzo.

(Español) Renuncia

LA INFORMACION QUE CONTIENE EL PRESENTE MANUAL ESTA SUJETA A CAMBIOS SIN PREVIO AVISO EN CUALQUIER MOMENTO.

Matrox Graphics Inc. se reserva el derecho de realizar modificaciones en cualquier momento y sin previo aviso. La información facilitada en este documento se considera que es exacta y fiable hasta la fecha de publicación. Sin embargo, Matrox Graphics Inc. no asume ninguna responsabilidad por su uso, por su reproducción y/o distribución parcial o total; ni por cualquier infracción de patentes u otros derechos de terceras partes derivados de su uso. No se concede ninguna licencia bajo cualesquiera patentes o derechos de patentes de Matrox Graphics Inc.

Compliance statements

USA

FCC Compliance Statement

Remark for the Matrox hardware products supported by this guide This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

WARNING Changes or modifications to this unit not expressly approved by the party responsible for the compliance could void the user's authority to operate this equipment. The use of shielded cables for connection of the monitor to the card is required to meet FCC requirements.

CANADA

(English) Innovation, Science and Economic Development Canada

Remark for the Matrox hardware products supported by this guide These digital apparatus does not exceed the Class A limits for radio noise emission from digital devices set out in the Radio Interference Regulation of Innovation, Science and Economic Development Canada.

(Français) Innovation, Sciences et Développement économique Canada

Remarque sur les produits matériels Matrox couverts par ce guide Ce present appareil numérique n'émet aucun bruit radioélectrique dépassant les limites applicables aux appareils numériques de Classe A prescrites dans le Règlement sur le brouillage radioélectrique édicté par Innovation, Sciences et Développement économique Canada.

UNITED KINGDOM

United Kingdom user's information – Declaration of Conformity

Remark for the Matrox hardware products supported by this guide These devices comply with Directive UK SI 2016 No. 1091 relating to electromagnetic compatibility for a Class A digital device. They have been tested and found to comply with EN55032/CISPR32 and EN55035/CISPR35. In a domestic environment these products may cause radio interference in which case the user may be required to take adequate measures. To meet UK requirements, shielded cables must be used to connect the monitor and other peripherals to the card. These products have been tested in a typical class A compliant host system. It is assumed that these products will also achieve compliance in any class A compliant system.

JAPAN

VCCI Compliance Statement

Remark for the Matrox hardware products supported by this guide This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

この装置は、クラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。　　VCCI－A

KOREA

A 급 기기 (업무용 방송통신기자재)

이 기기는 업무용 (A 급) 전자파적합기기로서 판 매자 또는 사용자는 이 점을 주의하시기 바라 며 , 가정외의 지역에서 사용하는 것을 목적으 로 합니다 .

EUROPE

(English) European user's information – Declaration of Conformity

Remark for the Matrox hardware products supported by this guide These devices comply with EC Directive 2014/30/EU for a Class A digital device. They have been tested and found to comply with EN55032/CISPR32 and EN55035/CISPR35. In a domestic environment these products may cause radio interference in which case the user may be required to take adequate measures. To meet EC requirements, shielded cables must be used to connect the monitor and other peripherals to the card. These products have been tested in a typical class A compliant host system. It is assumed that these products will also achieve compliance in any class A compliant system.

(Français) Informations aux utilisateurs Européens – Déclaration de conformité

Remarque sur les produits matériels Matrox couverts par ce guide Ces unités sont conformes à la directive communautaire 2014/30/EU pour les unités numériques de classe A. Les tests effectués ont prouvé qu'elles sont conformes aux normes EN55032/CISPR32 et EN55035/CISPR35. Le fonctionnement de ces produits dans un environnement résidentiel peut causer des interférences radio, dans ce cas l'utilisateur peut être amené à prendre les mesures appropriées. Pour respecter les impératifs communautaires, les câbles de connexion entre le moniteur ou autres périphériques et la carte doivent être blindés. Ces produits ont été testés dans un système hôte typique compatible classe A. On suppose qu'ils présenteront la même compatibilité dans tout système compatible classe A.

(Deutsch) Information für europäische Anwender – Konformitätserklärung

Anmerkung für die Matrox Hardware-Produktunterstützung durch dieses Handbuch Diese Geräte entsprechen EC Direktive 2014/30/EU für ein digitales Gerät Klasse A. Sie wurden getestet und entsprechen demnach EN55032/CISPR32 und EN55035/CISPR35. In einer Wohnumgebung können diese Produkte Funkinterferenzen erzeugen, und der Benutzer kann genötigt sein, entsprechende Maßnahmen zu ergreifen. Um EG-Anforderungen zu entsprechen, müssen zum Anschließen des Monitors und anderer Peripheriegeräte an die Karte abgeschirmte Kabel verwendet werden. Diese Produkt wurden in einem typischen, der Klasse A entsprechenden, Host-System getestet. Es wird davon ausgegangen, daß diese Produkte auch in jedem Klasse A entsprechenden System entsprechend funktionieren.

(Italiano) Informazioni per gli utenti europei – Dichiarazione di conformità

Nota per i prodotti hardware Matrox supportati da questa guida Questi dispositivi sono conformi alla direttiva CEE 2014/30/EU elativamente ai dispositivi digitali di Classe A. Sono stati provati e sono risultati conformi alle norme EN55032/CISPR32 e EN55035/CISPR35. In un ambiente domestico, questi prodotti possono causare radiointerferenze, nel qual caso all'utente potrebbe venire richiesto di prendere le misure adeguate. Per soddisfare i requisiti CEE, il monitor e le altre periferiche vanno collegati alla scheda grafica con cavi schermati. Questi prodotti sono stati provati in un tipico sistema host conforme alla classe A. Inoltre, si dà per scontato che questi prodotti acquisiranno la conformità in qualsiasi sistema conforme alla classe A.

(Español) Información para usuarios europeos – Declaración de conformidad

Observación referente a los productos de hardware de Matrox apoyados por este manual Estos dispositivos cumplen con la directiva de la CE 2014/30/EU para dispositivos digitales de Clase A. Dichos dispositivos han sido sometidos a prueba y se ha comprobado que cumplen con las normas EN55032/CISPR32 y EN55035/CISPR35. En entornos residenciales, estos productos pueden causar interferencias en las comunicaciones por radio; en tal caso el usuario deberá adoptar las medidas adecuadas. Para satisfacer las disposiciones de la CE, deberán utilizarse cables apantallados para conectar el monitor y demás periféricos a la tarjeta. Estos productos han sido sometidos a prueba en un típico sistema anfitrión que responde a los requisitos de la clase A. Se supone que estos productos cumplirán también con las normas en cualquier sistema que responda a los requisitos de la clase A.

EUROPE

(English) European user's information – Directive on Waste Electrical and Electronic Equipment (WEEE)

Please refer to the Matrox Web site (https://video.matrox.com/en/environment/product-waste-management) for recycling information.

(Français) Informations aux utilisateurs Européens – Règlementation des déchets d'équipements électriques et électroniques (DEEE)

Se référer au site Web de Matrox (https://video.matrox.com/en/environment/product-waste-management) pour l'information concernant le recyclage.

(Deutsch) Information für europäische Anwender – Europäische Regelungen zu Elektro- und Elektronikaltgeräten (WEEE)

Bitte wenden Sie sich an der Matrox-Website (https://video.matrox.com/en/environment/product-waste-management) für Recycling-Informationen.

(Italiano) Informazioni per gli utenti europei – Direttiva sui rifiuti di apparecchiature elettriche ed elettroniche (RAEE)

Si prega di riferirsi al sito Web Matrox (https://video.matrox.com/en/environment/product-waste-management) per le informazioni di riciclaggio.

FRANCE

Avertissement sur l'épilepsie

À lire avant toute utilisation d'un jeu vidéo par vous-même ou votre enfant Certaines personnes sont susceptibles de faire des crises d'épilepsie ou d'avoir des pertes de conscience à la vue de certains types de lumières clignotantes ou d'éléments fréquents dans notre environnement quotidien. Ces personnes s'exposent à des crises lorsqu'elles regardent certaines images télévisées ou qu'elles jouent à certains jeux vidéo. Ces phénomènes peuvent apparaître alors même que le sujet n'a pas d'antécédent médical ou n'a jamais été confronté à une crise d'épilepsie.

Si vous-même ou un membre de votre famille avez déjà présenté des symptômes liés à l'épilepsie (crise ou perte de conscience) en présence de stimulations lumineuses, veuillez consulter votre médecin avant toute utilisation.

Nous conseillons aux parents d'être attentifs à leurs enfants lorsqu'ils jouent avec des jeux vidéo. Si vous-même ou votre enfant présentez un des symptômes suivants: vertige, trouble de la vision, contraction des yeux ou des muscles, perte de conscience, trouble de l'orientation, mouvement involontaire ou convulsion, veuillez immédiatement cesser de jouer et consultez un médecin.

Précautions à prendre dans tous les cas pour l'utilisation d'un jeu vidéo Ne vous tenez pas trop près de l'écran. • Jouez à bonne distance de l'écran de TV et aussi loin que le permet le cordon de raccordement. • Utilisez de préférence les jeux de vidéo sur un écran de petite taille. • Évitez de jouer si vous êtes fatigué ou si vous manquez de sommeil. • Assurez-vous que vous jouez dans une pièce bien éclairée. • En cours d'utilisation, faites des pauses de dix à quinze minutes toutes les heures.

matrox®

video