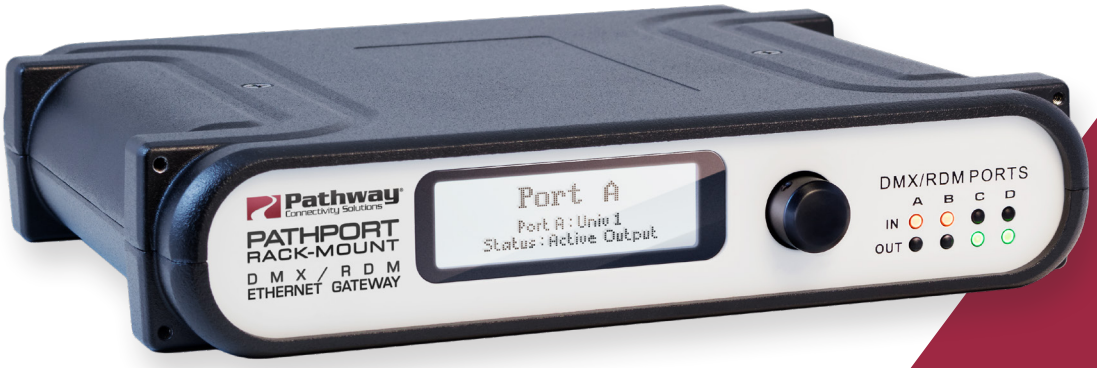
Pathport Rack-mount DMX/RDM Ethernet Gateway



Models PWPP RM P4

Running Firmware version 6.1 or later

User Guide

January 2023

Pathway® Connectivity Solutions

WARNING ABOUT UNSECURED PROTOCOLS

Enabling an open protocol that does not use encryption or authentication - These protocols could be eavesdropped or spoofed by malicious parties. You are strongly encouraged to use Pathway ssACN, and secure access to your network, both physically and technologically. To use unsecured protocols, you must acknowledge that you have read this statement and accept these risks.

CONTENTS

ABOUT PATHPORT RACK-MOUNT - PWPP RM P4

Pathway Connectivity's **PWPP RM P4** is a four-port DMX-over-Ethernet gateway intended for use primarily in entertainment lighting systems. The PWPP RM P4 provides transparent transmission and receipt of the DMX512 lighting control standard, using a number of widely accepted protocols including **Pathport Protocol, sACN (E1.31)**, **Art-Net**, **Strand ShowNet**, and **Pathway ssACN (Secure sACN)**, across a standard Ethernet data network.

The PWPP RM P4 may be used alone, networked with other PWPP RM P4 and Pathport gateways, as well as with a number of other Ethernet-aware lighting control products, such as consoles and controllers.

The PWPP RM P4, like all Pathports, is a routing device and does not provide control over the protocols or the data being passed. It only provides control over the path the data takes, how multiple DMX sources are treated (merged or prioritized), and certain other routing characteristics including DMX transmission speed and signal loss behavior.

The PWPP RM P4 is easily configured and upgraded using the freely available software tool, **Pathscape**. It is also configurable using the Front Panel UI, which consists of the LCD and rotary pushbutton encoder. **NOTE** that some features are not available if configuring the device solely with the front panel.

PROTOCOLS SUPPORTED

DMX512

The most widely used digital multiplex protocol for controlling entertainment lighting and effects equipment. The DMX signal consists of 512 8-bit control packets sent asynchronously over a two-pair shielded cable at 250K Baud. The standard connector type is 5 pin XLR. The standard has been revised several times over the years, with the latest being ANSI E1.11 DMX512-A (2013). The PWPP RM P4 is designed to work seamlessly with all variants of the protocol.

DMX is a last mile protocol, daisy-chained between end fixtures.

ETHERNET PROTOCOLS

Ethernet protocols are used to multiplex DMX data over Ethernet networks, largely to circumvent control channel limitations inherent in the DMX standard. The v supports the most widely accepted.

Pathport Protocol: A broadcast protocol developed by Pathway Connectivity and implemented by a variety of console manufacturers.

Art-Net: A broadcast protocol developed by Artistic Licence. Its free distribution has made in popular with media server manufacturers. Because this is not a standard, some implementations may not work with others.

Strand Shownet: A proprietary broadcast protocol developed by Strand Lighting and used exclusively in Strand lighting consoles.

ANSI E1.31 streaming ACN (sACN): A multicast industry standard developed and maintained by the Technical Standards Program of the Entertainment Services and Technology Association (ESTA). The standard is available for a nominal cost from ESTA. This standard provides the DMX512 data transport for the separate ANSI E1.17 ACN (Architecture for Control Networks) industry standard.

sACN is the DMX transport used by ETC Net3. The PWPP RM P4 is fully compliant with Net3, and will seamlessly receive either Final Draft 20, or the ANSI approved versions of sACN.

Pathway ssACN (Secure sACN): A new protocol developed by Pathway Connectivity that incorporates many features of ANSI E1.31 sACN, but adds a layer of secure authentication. See later in the manual for details on Pathway ssACN.

REMOTE DEVICE MANAGEMENT (RDM)

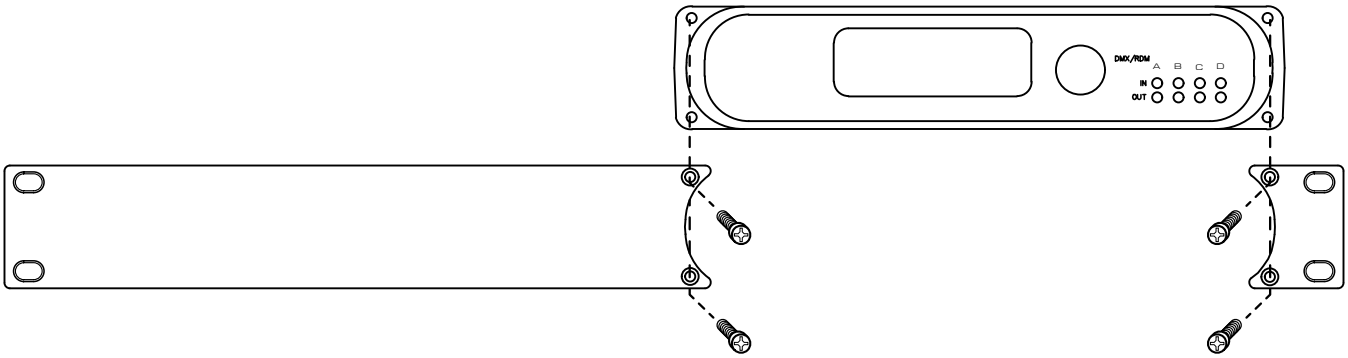
ANSI E1.20 Remote Device Management (RDM) is an industry standard, also published by ESTA, which allows remote configuration of last-mile DMX devices, using the same wire pair that carries the DMX signal. Like DMX, RDM requires a separate dedicated controller to generate the signal packets the PWPP RM P4 will route. The freely available Pathscape software is required to use the PWPP RM P4 as an RDM gateway to configure DMX-based equipment.

INSTALLATION INSTRUCTIONS

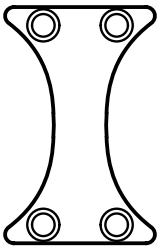
The PWPP RM P4 is intended for desktop use, or to be mounted in a standard 19” equipment rack, using the included rack ear accessories.

Rack ear accessories for installing the PWPP RM P4 into a 19” equipment rack. Long and short sections can be swapped to either side as needed.

Use the included machine screws (2 per side) to attach the rack ears to the either side of the metal chassis.



If mounting two PWPP RM P4 units together (or an eLink and a PWPP RM P4) use the rack ear coupler between the units to fit both into one rack space.

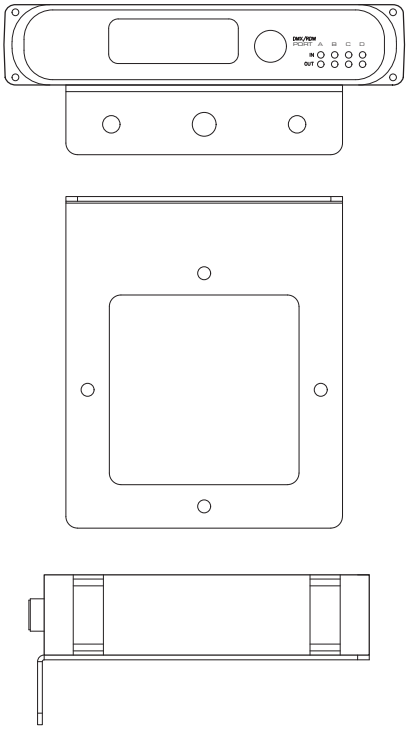


Rack ear coupler included with the PWPP RM P4 for attaching unit to another eLink or PWPP RM P4 in a 19” equipment rack

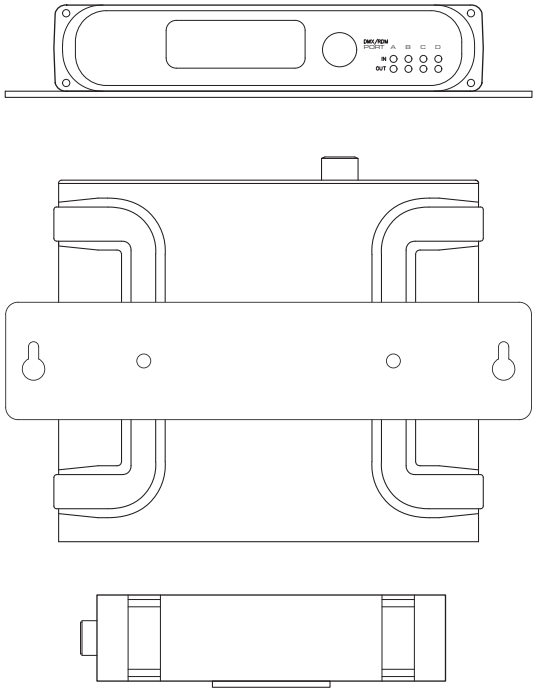
If using the PWPP RM P4 on a desktop permanently, you may wish to apply the adhesive rubber feet pads to the bottom of the unit. Simply peel them off the adhesive backing and apply to the bottom of the metal enclosure, with one on each corner.

OPTIONAL MOUNTING ACCESSORIES

Wall-mount kits (PWACC WMSM) and truss-mount adapters (PWACC TMSM) are available as accessories.



PWACC WMSM Wall-mount Kit



PWACC TMSM Truss-mount Kit

INSTALLATION ENVIRONMENT

The PWPP RM P4 is intended for installation in a dry, indoor location. Ambient operating conditions are **14°F to 122°F (-10°C to 50°C); 5-95% relative humidity, non-condensing.**

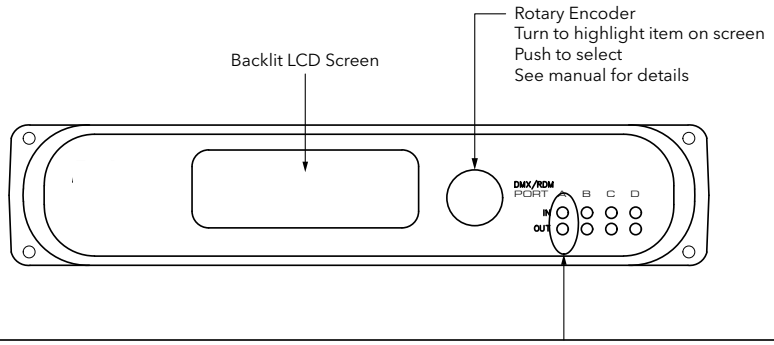
Warning: If using a 24-48VDC power supply, its AC socket outlet shall be installed near the equipment and shall be easily accessible.

Warning: This equipment relies on building installation primary overcurrent protection.

Warning: Except for the chassis plug marked for 24-48VDC input, all ports on the PWPP RM P4 are intended for low voltage and/or data lines only. Attaching anything other than low voltage sources to the data ports may result in severe equipment damage, and personal injury or death.

PANEL LAYOUTS

FRONT PANEL



LED Indicator Chart - Indicators apply on a port-by-port basis			
Color	Label	Action	Explanation
AMBER	INPUT	Flashing	No Data Present
		Steady On	Valid DMX Received
GREEN	OUTPUT	Flashing	No Data Present
		Steady On	Valid DMX Transmit

LCD

Front-panel LCD shows device name, IP address, status, and menus, when configuring settings with the rotary encoder. The LCD backlight will come on when the encoder knob is being used, but can be permanently enabled using Pathscape.

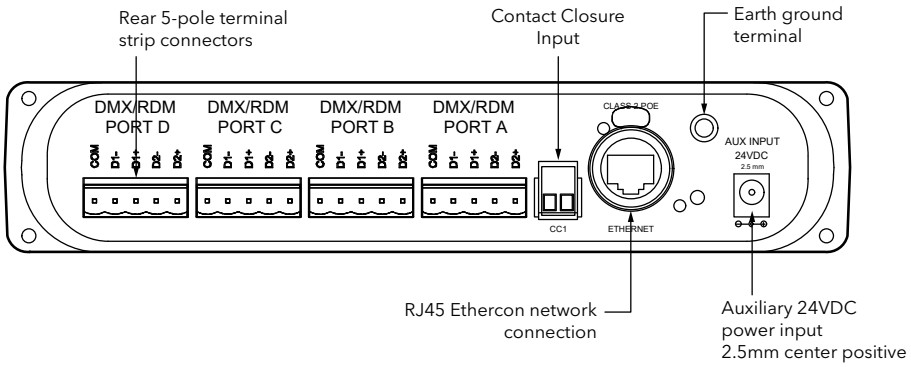
ROTARY ENCODER

Push-button rotary knob is used to check and set device settings. Rotate the knob to select different menus and options, push in the knob to make a selection.

LED INDICATORS

See the chart above for details.

REAR PANEL



PWPP RM P4 TERM REAR Shown

DMX PORTS

Depending on the model number ordered, the DMX ports are: 5-pin XLR, RJ45 etherCON connectors or terminal strip connectors. The XLR and etherCON connectors are of the locking type.

Plug your DMX512-capable devices into these ports using the appropriate cables. To unplug XLR and etherCON connectors, push in the tab labeled “PUSH” at the top of the connector to unlock, then pull out the connector.

RJ45 etherCON NETWORK CONNECTION

Plug the PWPP RM P4 into the lighting network using an Ethernet cable here. The Link/Act LED will light up amber when a link is established, and will flash when there is network activity. If the LED is off, there is no active link.

If using PoE, connect the PWPP RM P4 to a PoE switch.

CCI (CONTACT CLOSURE INPUT)

There is a dry contact closure input on the rear panel. Shorting the two terminals will activate the associated function. The Contact Closure can activate DMX Hold, RDM Pause, and more functions may be added in future firmware updates.

POWER CONNECTIONS

The PWPP RM P4 can be powered via a Power-over-Ethernet (PoE) source, such as a Pathway VIA PoE Switch. The PoE source must be connected to the Ethernet Port.

The PWPP RM P4 may be powered via DC Power supply between 24-48 VDC, center positive, 2.5mm barrel connector. A screw terminal is provided to connect the device to earth ground.

CONFIGURATION

The PWPP RM P4 may be configured from the front panel interface using the LCD and rotary pushbutton encoder. However, we recommend using our free software tool, Pathscape. To download Pathscape, visit the Pathway website.

For instructions on how to set properties and send transactions to devices, refer to the Pathscape manual.

For instructions on using the LCD and encoder to navigate the switch menus, see the **Front Panel UI and Menu** section.

SECURITY

BACKGROUND INFORMATION

On **January 1, 2020**, California became the first state to enforce cybersecurity and IoT related legislation. Oregon, New York and Massachusetts are following suit. California's law is Title 1.81.26 "Security of Connected Devices" and mandates that we equip our products with security features that are appropriate to the nature and function of the device. By law, this encompasses all products that are assigned Internet Protocol addresses which can connect to the Internet directly or indirectly. Pathway Connectivity, a division of Acuity Brands, will only ship compliant devices regardless of the jurisdiction into which they are sold.

The law requires us to either supply a unique password for our products (see **Local Configuration Only** below) or requires the users to change the password before being able to use it (See **Creating a Security Domain** below). With Pathscape V3 and later, we provide features that protect our products from unauthorized access or use by enforcing passwords.

Pathway Connectivity does not collect or store personal information on our devices.

WHAT THIS MEANS TO YOU

1. When using products shipped after January 1, 2020, Pathscape will require a single password to allow configuration of all the devices on your network. Since the release of Pathscape V4, all Pathway Connectivity products can be upgraded to firmware version 6.x. It is suggested you upgrade your devices to take advantage of the most recent security improvements.

2. Products shipped before January 1, 2020, devices with version 3.x and 4.x firmware will continue to function without passwords using either Pathscape version 3 or 4.

3. All products shipped after January 1, 2020 may only be configured using Pathscape 4 or later.

4. Products shipped after January 1, 2020 cannot be downgraded to earlier password-free firmware.

   Using the **Tools >**  **Firmware Updater** dialog (see later in the manual for instructions), devices manufactured before January 1, 2020 may show newer firmware versions, but using the **Select Latest** button will not select the latest. These devices do not have a method, like a front panel, to factory default them. You can manually select the latest firmware using the **Select Firmware** button, but do **not forget the new password** as you cannot factory default them.

   We highly recommend printing the Password Recover PDF when creating a Security Domain so you can reset lost passwords.

5. Products that are fully configurable from the front panel can enter **Local Configuration Mode** (**Read-Only mode**). This allows them to be configured locally, but not over the network.

6. You will be encouraged to print or save a recovery key in case you lose the password. Do so when setting up your Security Domain. It is the **only chance** you'll get to save/print/see this Recovery Key.

7. If you lose the password and lose the recovery key, you will manually have to factory default each device on the network. See the resource section of the Pathway website for a comprehensive document describing how to manually factory default all our devices.

8. The complete network configuration may be saved without a password before factory defaulting devices. Applying the saved configuration will require a new password to be set for the network.

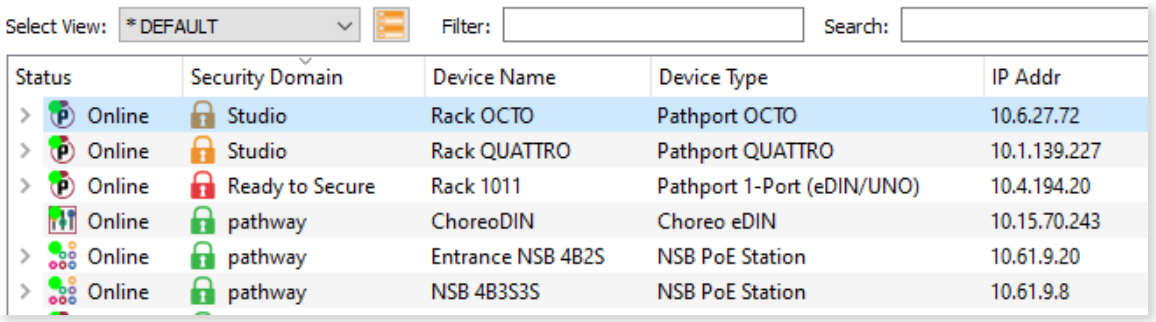
9. Configuring our devices to receive unsecured protocols such as sACN and Art-Net will require you to accept the risks. **See WARNING BOX regarding unsecured protocols below.**

   By default, all Pathway Connectivity products sent and/or receive Pathway ssACN which is an authenticated method of transporting the E1.31 protocol within a Security Domain.

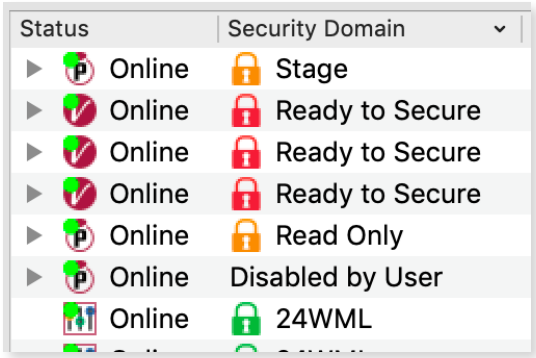
10. Pathway does not store personal information such as names or email addresses on our devices.
11. On products with a front panel display and encoder using firmware release 6.1, it is possible to opt out of the prescribed security features. See **Disabling Security** below.

SECURITY DOMAINS

To simplify the process of managing security on your network, Pathscape introduced the concept of a "**Security Domain**". Below we will describe how to create a Security Domain and add or remove devices from it. In the **Device** tab of Pathscape there is a column that shows you the name of the devices' domain and a **padlock icon** showing their current state.



There are several different ways a device can appear in the **Security Domain** column.



RED PADLOCK - "Ready to Secure" device (previously "Unsecured")

Prior to Pathscape version 4.1, this was shown as "**Unsecured**".

Any device shipped after **January 1, 2020** will have version 5 or later firmware which includes security. These devices will report their type, name and firmware version **only**. All other properties cannot be read until you add them to a Security Domain (see below on creating domains).

AMBER PADLOCK - "Other Domain" name showing device

Devices that have been added to a security domain will appear with an amber padlock. These devices will allow you to read all their properties and even save a show file with the network setup, but the properties are Read-Only. You will have to login to the domain to set any properties. (See **Login procedure** below.)

AMBER PADLOCK - "Read Only" (previously "Locally Secured")

Prior to Pathscape version 4.1, this was shown as "**Locally Secured**".

Read Only means the front panel was used to create a unique (and hidden) password to allow front-panel-only configuration.

To gain read/write privileges with Pathscape, you **must Reset Security** settings from the front panel and then add it to the Security Domain using Pathscape.

GREEN PADLOCK - “My Domain” shows devices in the current domain

Once you have logged into a Security Domain with a password, any device in your domain will appear with a green padlock and all their properties will be Read/Writable.

NO PADLOCK - “Disabled By User” – Firmware version 6.1 or later - rackmount devices with front panel UI only

With the release of **firmware version 6.1 for rackmount devices with a front panel display and encoder (PWPP RM P8, PWPP RM P4, PWVIA RM only)**, it is possible to opt out of the security features altogether. This is designed primarily for the rental market where devices may be shipped to various locations for use by different end users, where Domain passwords and Recovery Keys may not be known.

Devices set to **Disabled by User** will behave like legacy devices and are fully Read/Writable by Pathscape without needing to be logged into a Domain.

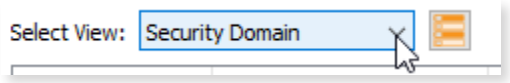
For information on opting out of security features, see **Disabling Security** below.

EMPTY SECURITY DOMAIN CELL – Firmware version prior to 5.0 - device shipped prior to January 1, 2020

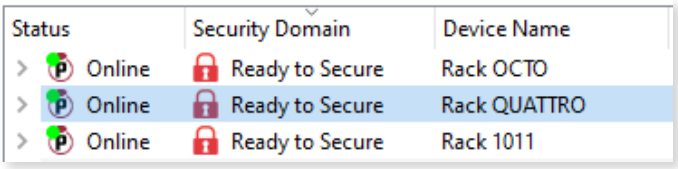
If the Security Domain cell is empty, this device is using Version 4 firmware and cannot be secured. Pathscape 4 will be able to read and write properties exactly like earlier versions of Pathscape. If you upgrade to version 5 or later firmware, the device will appear with a red padlock and you will need to add it to a domain before you can use it.

CREATING A SECURITY DOMAIN

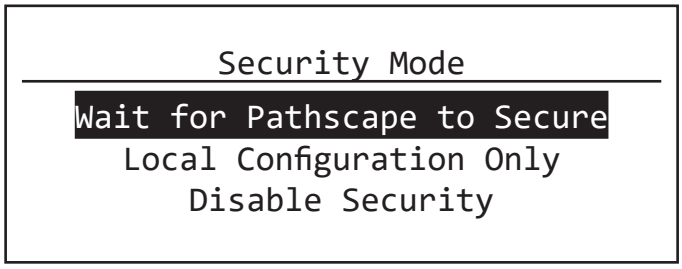
- After starting Pathscape, the online devices will populate the Device View.
- Choose the **Security Domain** view from the **Select View** dropdown

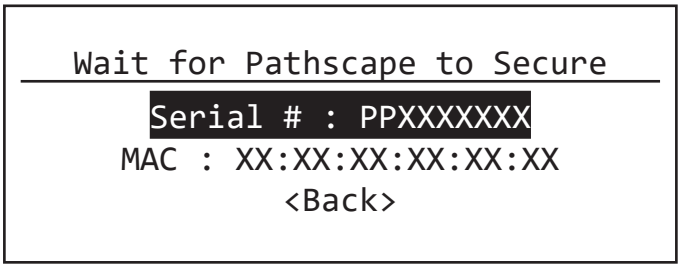


- Each device running V5 or later firmware will have a **Red "Ready to Secure"** value in the **Security Domain** column.



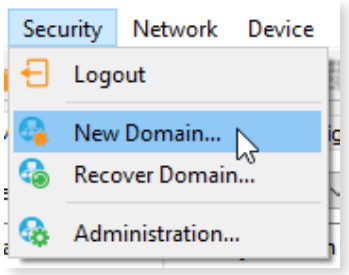
- **NOTE**: PWPP RM P4s running **V6.1 firmware or later** will show a **Security Mode** screen on the front panel LCD.

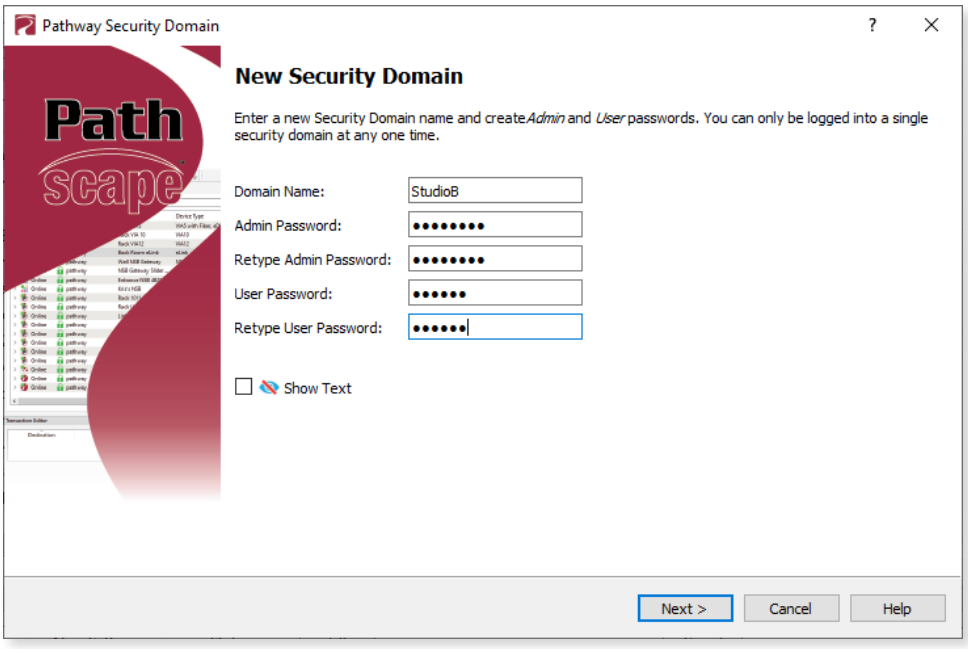




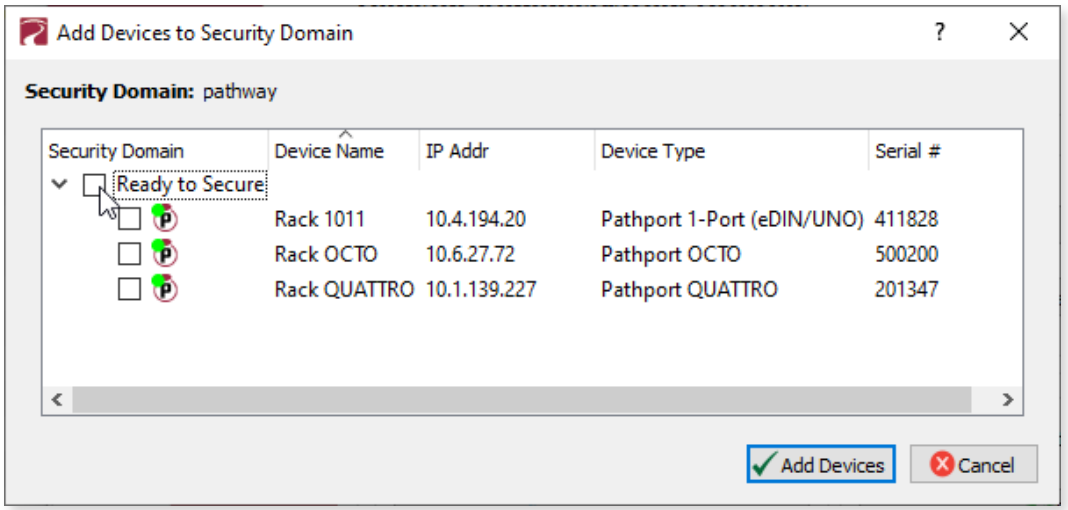
- **No action is required** here to add the device to Pathscape. Clicking the encoder knob to select **Wait for Pathscape to Secure** will show the device Serial Number and MAC Address, in cases where this may be helpful for device identification.
- If you want to configure your devices only via the front panel, choose **Local Configuration Only**. If you prefer to opt out of security and the needs for passwords on these devices, choose **Disable Security**.

  See the below for more detail on these options.
- If your devices have old firmware, you may update them to current firmware by going to the **Tools** menu in Pathscape and selecting **Firmware Updater**. Select the devices to upgrade, and choose **Select Latest**, then **Send Firmware**. (See the **Upgrading Device Firmware** section for more detail). The devices will go offline and come back with a **red padlock**.
- From the **Security** menu, choose **New Domain.**





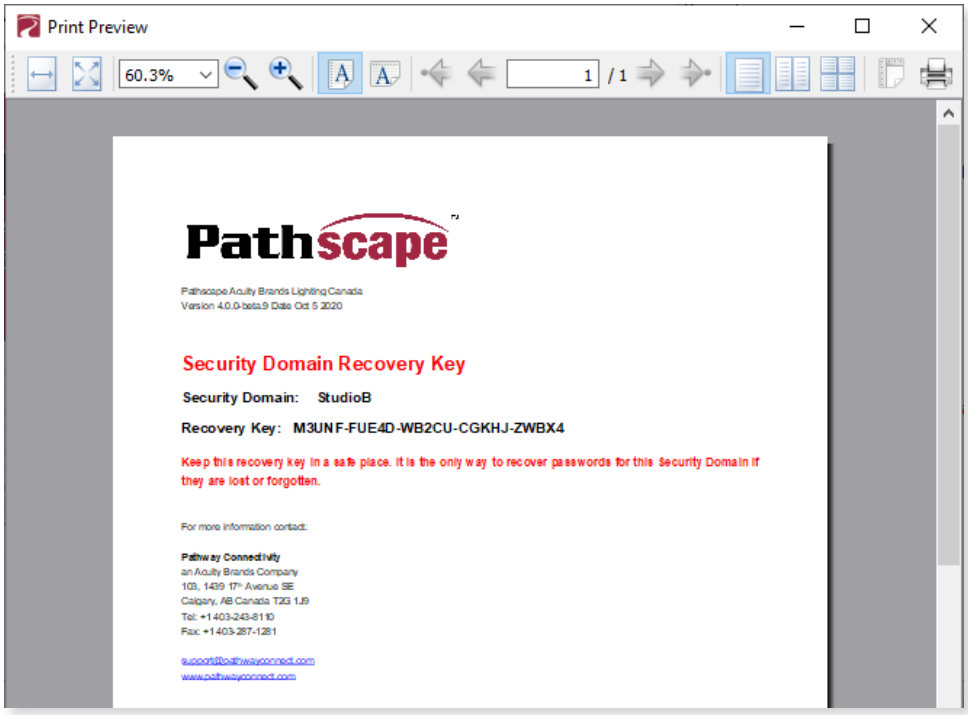
- Enter the new **Domain Name** and **Administrator** and **User passwords**, then click **Next.**
  - The **Administrator** can change passwords, change the Security Domain's name, factory default devices, manage Device Restore Points and add or remove devices from the domain.
  - The **User** can change device properties and save and restore show files, but cannot change domain passwords, factory default devices or add/remove devices. There is one User account password for all users.
- Add all the Ready to Secure devices on your network by checking the top checkbox labeled "**Ready to Secure**" and then click **Next**. If you wish to add some but not all devices to this domain, click on the checkbox next to each device you'd like to add, and then click **Add Devices**.



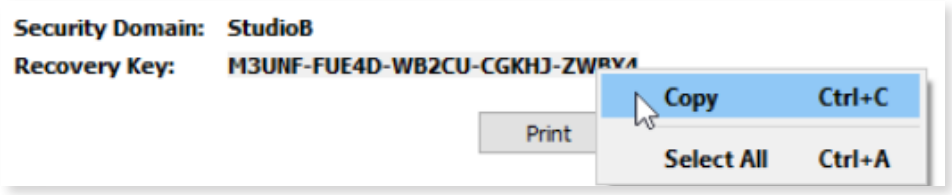
- The next window will show the **Recovery Key**. This key will allow you to recover Security Domain access should the passwords be lost or forgotten.

  It is extremely important to keep a record of this Recovery Key, as this is the only time it will be shown to you. Print the Recovery Key.

- Clicking the **Print** button will open a Print Dialog, from which you may choose a printer to print to.

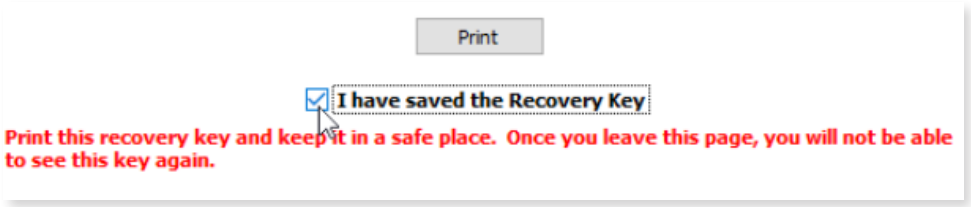


- You may also right-click on the Recovery Key, then **Select All** and **Copy** the key to the clipboard and store it in a safe place.

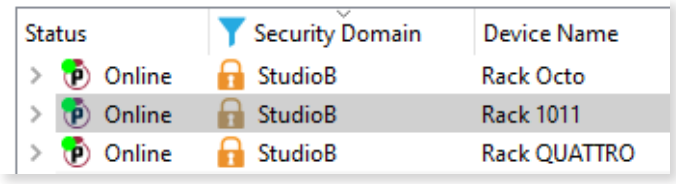


- In order to proceed, you **must click the checkbox** acknowledging you have printed or saved the Recovery Key in some way.

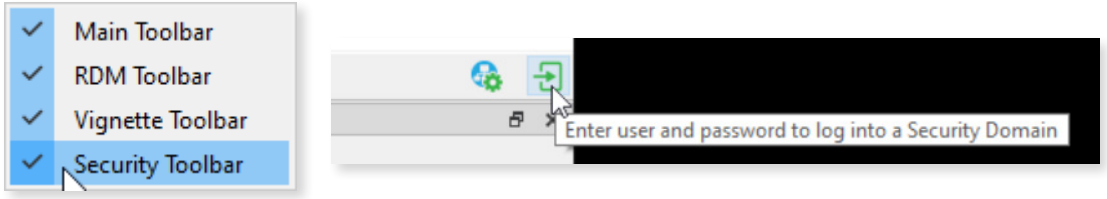
  Managers of the facility should store this key in a safe place, keeping in mind that anybody with this key can change both the Administrator and User passwords at any time.



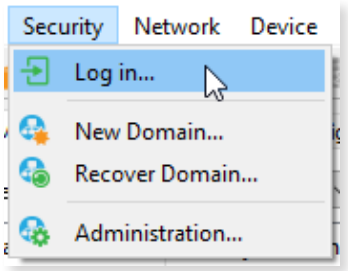
- Click **Finish** and the window will close, and the devices will be added to the domain. The devices will have an **amber padlock** and their properties will be read-only.



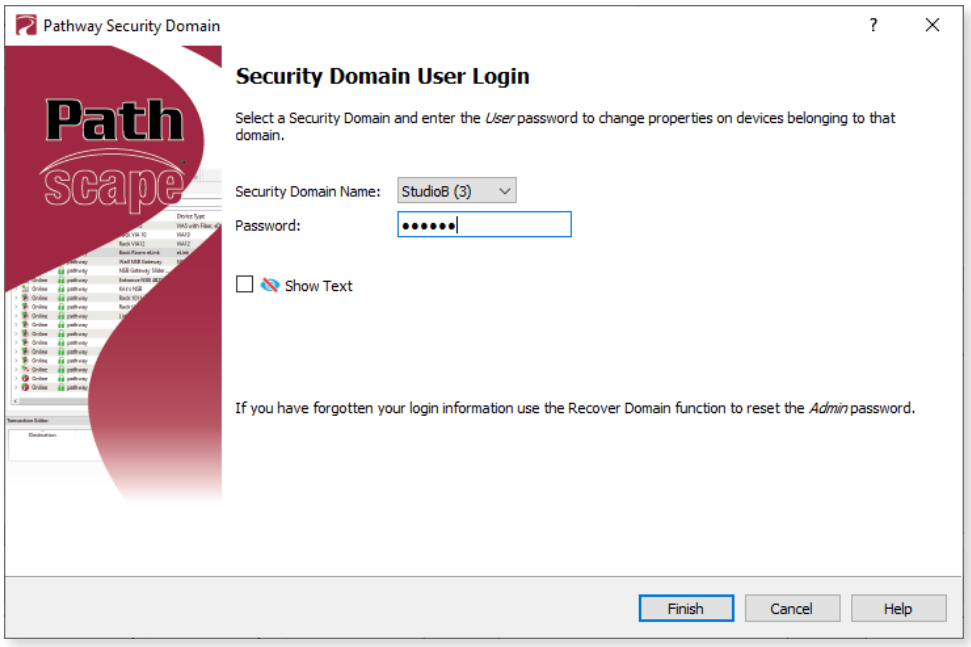
- To configure the devices, you must log in to the domain **as a user** by pressing the Log In button in the toolbar. **Note**: The **Security Toolbar** option under the **Window** menu must be checked.



You can also click on the **Security** menu and select the Log In menu item.

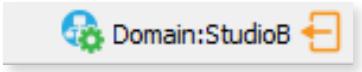


- Enter the **User** password for the Security Domain that was just created, and click **Finish**.



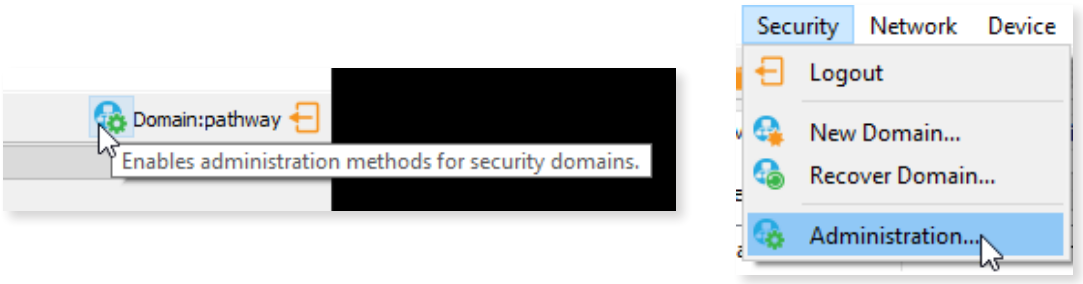
As security parameters are verified, the amber padlocks will turn **green** and the properties of those devices will be read/writable.

Once logged into a domain, the **Log In** button will change to the **Log Out** button, and the name of the domain currently logged into will appear next to it.

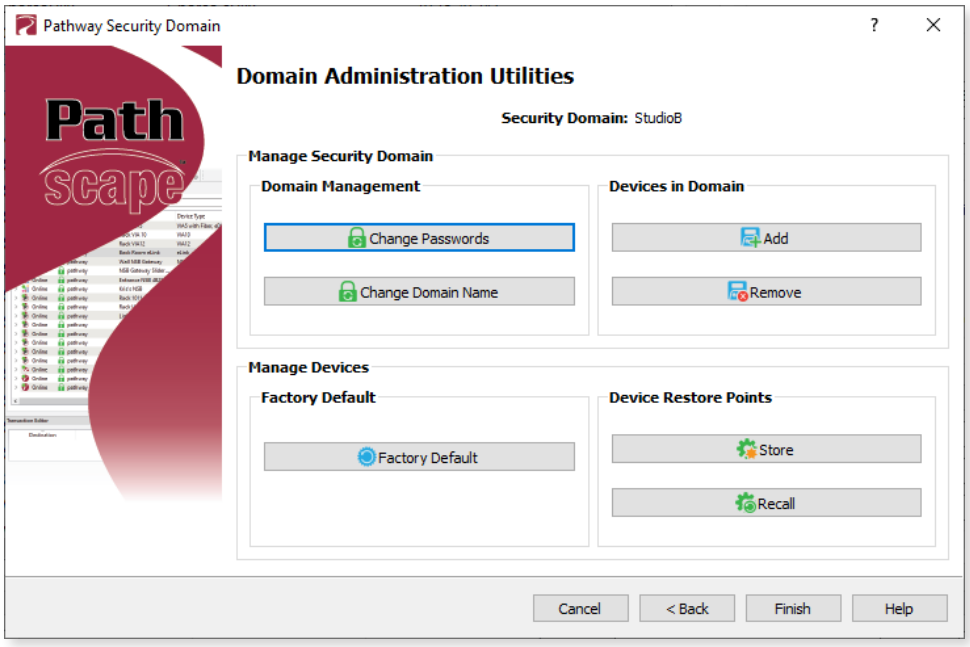


ADMINISTERING A DOMAIN

To administer a domain, click on the **Administration** button on the Security Toolbar, or click the **Security** menu and select **Administration**.



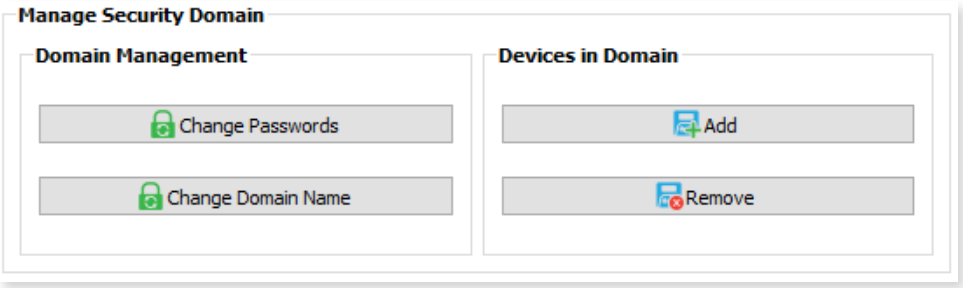
Enter the **Admin** password for the Security Domain, and the **Domain Administrator Utilities** window will appear.



The Domain Admin Utilities window is broken down into to main sections, **Manage Security Domain** and **Manage Devices**.

MANAGE SECURITY DOMAIN

This section is broken down further into functions that relate to **Domain Management**, including Domain Name and Passwords, and **Devices in Domain**, which allows you to add and remove devices in the Domain.



DOMAIN MANAGEMENT

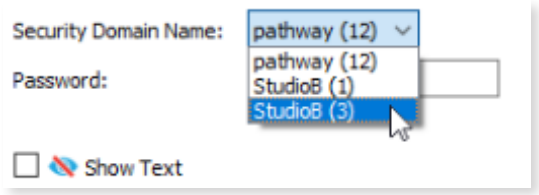
CHANGE PASSWORDS

If your staffing changes, it is a good idea to change the passwords on the domain. Click this button to change the current Security Domain Admin and User passwords. **All devices should be online when you change the password.**

Once you have entered both Admin and User passwords, click the **Change Passwords** button to confirm the changes.

Note: Changing the domain passwords does not generate a new Recovery Key. The original key is still valid, as it is only generated at the time of the Domain's creation.

Note: **If some devices are offline and you change the password**, when those devices come back online, they will coincidently have the same domain name, but will be using the old password. When logging in, there will be two domains with the same name.



You will have to remove the devices on the old domain, then add them to the new domain using the new password. You can remove them using the **Remove** button in the **Domain Administration Utilities** menu (see below for details).

The number in parentheses after the domain name is the number of devices that are in that domain. In the example above, there are 12 devices in the "pathway" domain.

This will help you identify which is the old domain. Log into the old domain using the old password and remove the devices. When they come back online, they will appear as **Ready to Secure**. Add them to the new domain using the new password.

CHANGE DOMAIN NAME

Click this button to change the name of the current Security Domain.

Enter a new name for the current domain, and click **Change Domain Name**.

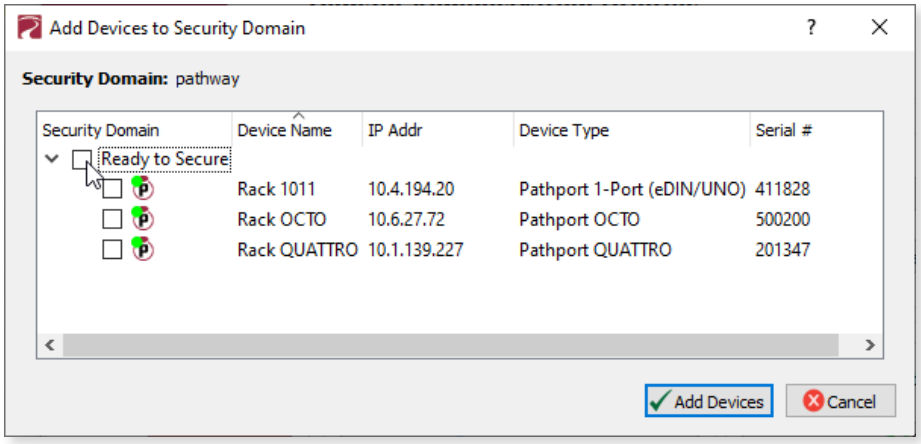
The window will close, and you will be logged out of the current domain, and the Domain Name will be changed to the new value. **You will have to log into the Domain again** to make any further changes.

Note that changing the domain name **does not** generate a new Recovery Key. The original key is still valid, as it is only generated at the time of the domain's creation.

DEVICES IN DOMAIN

ADD

Clicking on this button will bring up the **Add Devices** window, where Ready to Secure devices can be added to the current Security Domain.

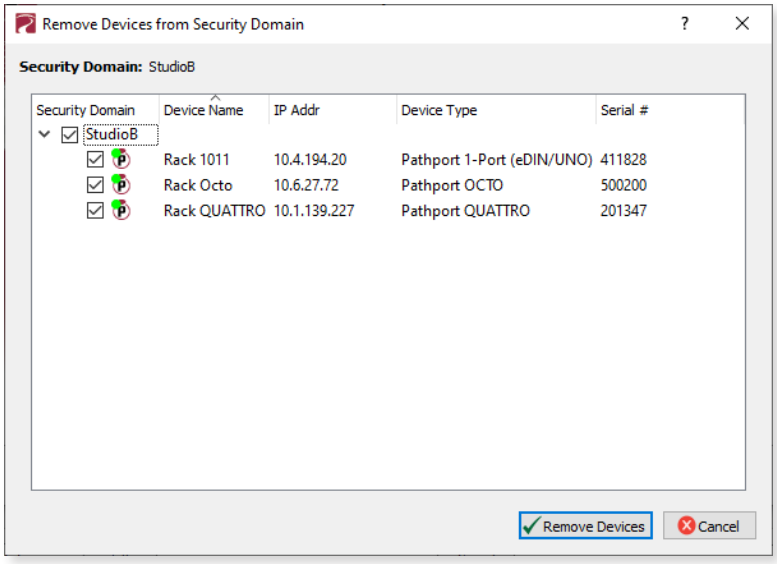


Click on the checkboxes next to the devices you want to add to the Domain, and click the **Add Devices** button. To add

all the listed devices, click the top checkbox next to “Ready to Secure” which will auto-check all the devices’ checkboxes.

REMOVE

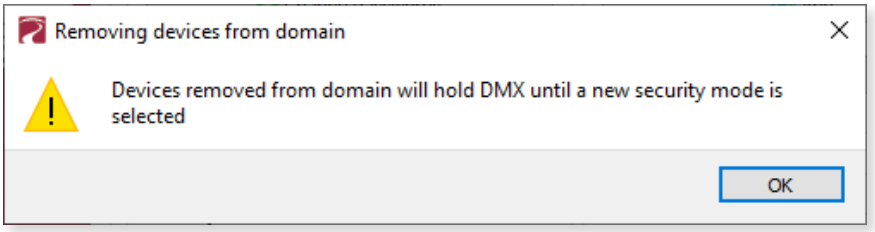
Click this button to remove devices from the current Security Domain.



Click on the checkboxes next to the devices you want to remove from the Domain, and click the **Remove Devices** button. To remove all the listed devices, click the top checkbox next to the Domain Name which will auto-check all the devices’ checkboxes.

The devices will then be removed from the Security Domain, and will appear as **Ready to Secure**. The devices can then be added to another domain as needed.

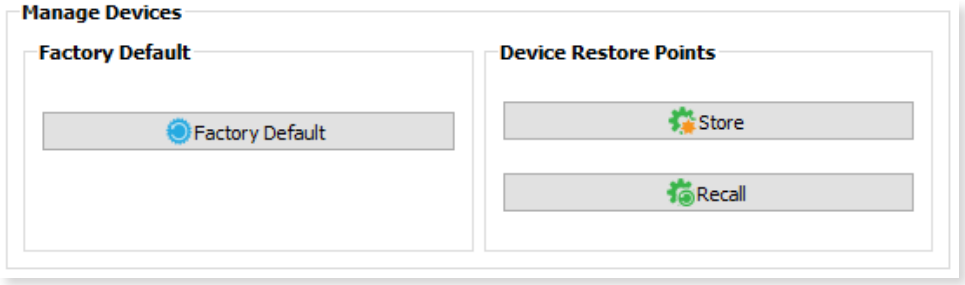
Note: When a device is removed from a domain, a window will appear reminding you that any active Network DMX levels will be held by that device until a new security mode is selected.



If all devices in a domain are removed from the domain, that domain is then deleted. This action cannot be undone. If you remove all devices from a domain and then want to add devices back to that domain, you will have to create a new domain with the same name, copy down the new Recovery Key, and add those devices again. **NOTE**: The original Recovery Key is now useless.

MANAGE DEVICES

This section is broken down further into functions that relate to **Factory Defaulting** devices as well as setting or restoring **Device Restore Points**.



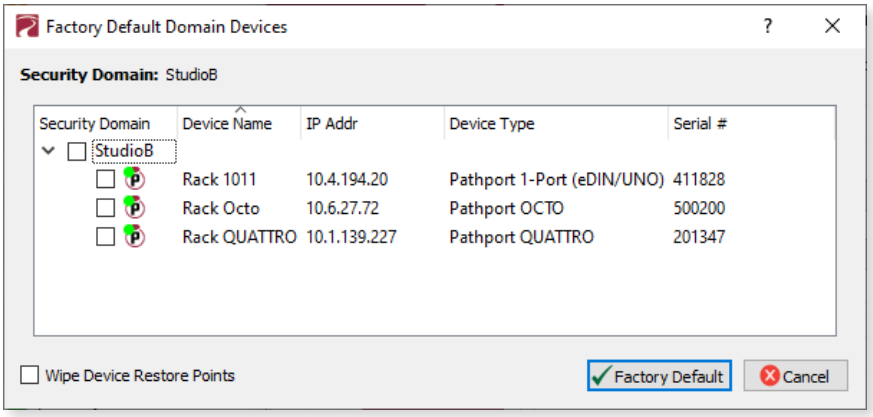
FACTORY DEFAULT

FACTORY DEFAULT

If you want to clear the settings of a device and return it to the factory defaults, click **Factory Default**.

Note that only devices in the Security Domain shown in this dialog box will be available to be defaulted. For devices running firmware V4 or below or devices that opted out of security, select the device and choose Factory Default in the Device menu.

See the Pathway website under **Support > Reference Articles > Factory Defaulting Ethernet Devices** for detailed instructions.



At the bottom of the window, you may optionally **Wipe Device Restore Points** from all checked devices. See below for details on Device Restore Points.

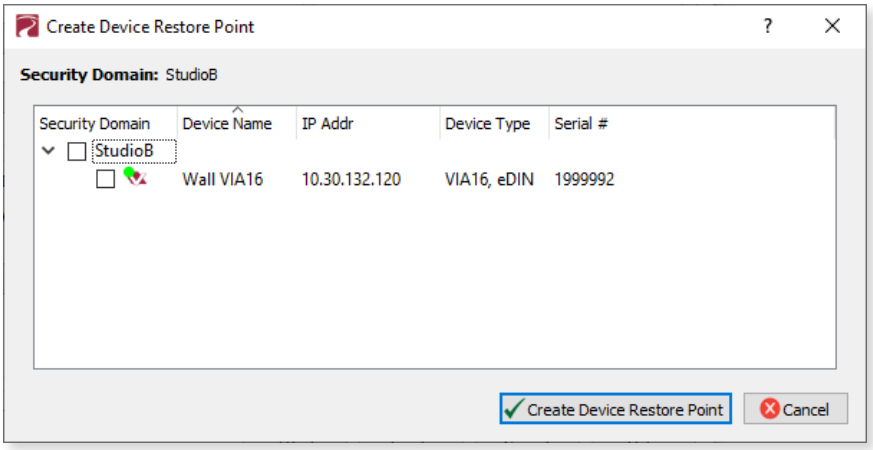
DEVICE RESTORE POINTS

With the release of firmware V6.0, certain Pathway products (PWVIA Switches including models PWVIA RM P12 RJ45EC NONPOE, PWVIA RM P12 RJ45EC POE, PWVIA RM P12 DUO POE and PWVIA RM P12 QUAD POE; Pathport gateways including PWPP RM P8, PWPP RM P4, PWPP DIN P4, PWELINK RM P2 RJ45EC REAR and PWGW DIN CLK) will support Device Restore Points.

Creating a Device Restore Point saves the device's current configuration and settings to its internal memory, for later recall. This differs from a Pathscape show file, in that the show file is saved on a PC running Pathscape.

STORE

Click this button to open the **Create Restore Point** window.

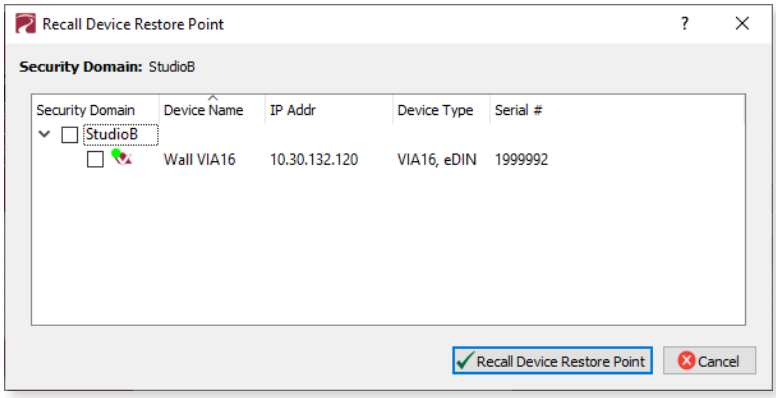


Click the checkbox next to each device on which you'd like to create a restore point. To check all devices, click the topmost checkbox. Click **Create Device Restore Point** to confirm.

Note that if there are no connected devices that support this feature, this button will be grayed out.

RECALL

Click this button to open the **Recall Restore Point** window.



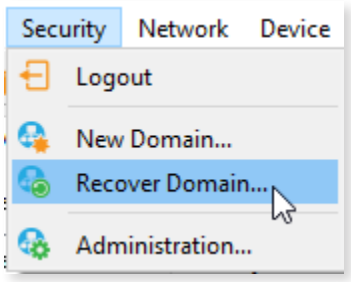
Click the checkbox next to each device on which you'd like to recall its restore point. To check all devices, click the topmost checkbox. Click **Recall Device Restore Point** to confirm.

Note that if there are no connected devices that support this feature, this button will be grayed out.

RECOVERING A DOMAIN

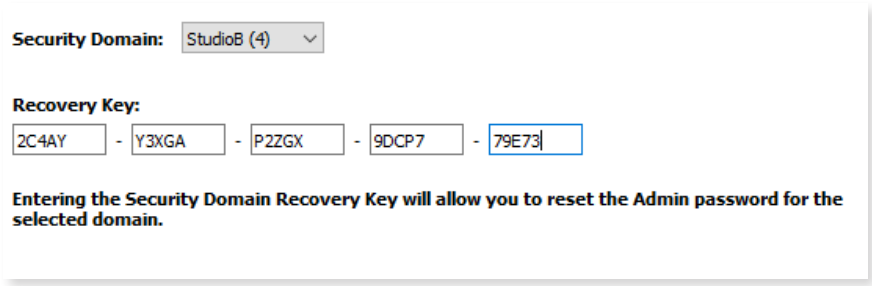
If you lose the Administrator password (or it was maliciously changed without your consent), you can recover the domain, retaining its configuration and set new passwords.

- From the menu, choose **Security >** **Recover Domain**.



- The **Reset Device Security** window will open.

- Type in the 25-digit **Recovery Key** and press **Next**.



- Type in a new **Administrator Password**, and click **Finish**.

- Now you can log into the **Domain Administration Utilities** Panel using the new Admin password you just specified. At this point you can set a new user password as well, using the **Change Passwords** button, as explained above.

RETAINING DEVICE SETTINGS FROM UNKNOWN DOMAINS

In the unlikely event that you don't know the password of a Security Domain, but you'd like to retain all its configuration, try the following:

Without logging in to a Domain, all devices that appear with amber padlocks are **read-only**. Save a show file, and the configuration of all devices is saved. You can then factory default the devices using the prescribed method.

See the Pathway website, under **Support > Reference Articles > Factory Defaulting Ethernet Devices** for detailed instructions.

Once they reappear in Pathscape as **Ready to Secure**, add them to a Security Domain and log in. Once all devices appear with a **Green Padlock**, open the show file and **Send All Transactions** to restore the network configuration and patch.

USING OLDER VERSIONS OF PATHSCAPE WITH NEW DEVICES

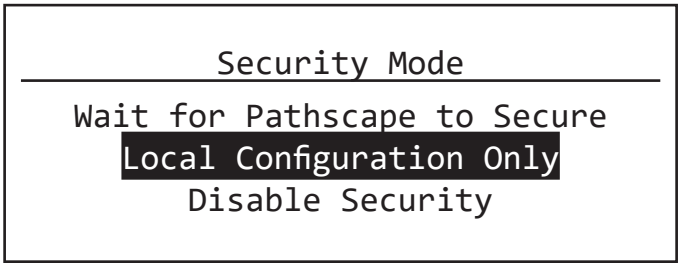
If you use Pathscape 1 or Pathscape 2 with devices shipped after **January 1, 2020 (Version 5 firmware or later)**, you will not be able to configure them. **You must use Pathscape 4 or later**. As a reminder, the device label will appear in the earlier versions of Pathscape as "**Use latest Pathscape PC software to secure**". Other properties will be shown and are correct, but any attempts to change them will fail.

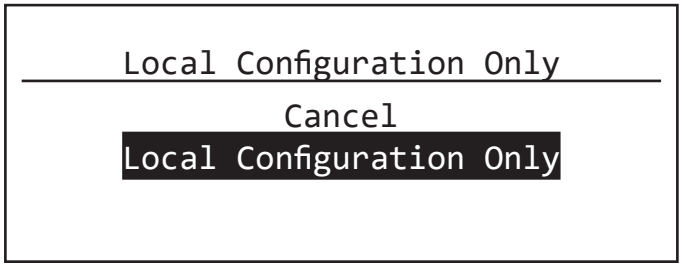
LOCAL CONFIGURATION ONLY - Using PWPP RM P4 without Pathscape

The PWPP RM P4 has features that use unsecured protocols. You may not intend to use Pathscape, but "bad actors" could potentially access the device and change the configuration. Therefore it is prudent to configure **Local Configuration Only** (Read Only) mode to protect your network if you want to use the PWPP RM P4, but are not using Pathscape to add your devices to a **Security Domain**.

Enter **Local Configuration** mode by selecting **Local Configuration Only** from the **Security Mode** menu.

This menu is shown upon bootup when no Security Mode has been set, i.e. when first received from the factory, or when the device has been factory defaulted or had its Security settings reset.





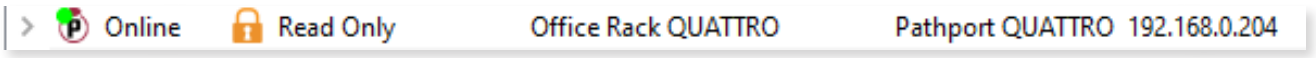
- From the **Security Mode** menu shown on the LCD, turn the encoder to select **Local Configuration Only**. In the submenu, confirm by selecting **Local Configuration Only** again. You will then have full access to the menus.
- In Local Configuration / Read Only mode, **Pathway ssACN** (Secure sACN) is not available. To use other standard (unsecured) protocols, you **must manually enable them**.

  In the **Protocol Support** menu, select the **Allow Unsecured RX** and choose **Accept the Security Risk** to enable unsecured protocols. **NOTE**: If you've disabled security (See **Disabling Security** below) the **Allow Unsecured RX** option is not available.
- Enable RX on the protocols you want to receive.
- On each port, set **Port Direction** to Input or Output and patch a standard universe (i.e., UNIV 1).

WARNING ABOUT UNSECURED PROTOCOLS

You are enabling an open protocol that does not use encryption or authentication. These protocols could be eavesdropped or spoofed by malicious parties. You are strongly encouraged to use Pathway ssACN, and secure access to your network, both physically and technologically. To use unsecured protocols, you must acknowledge that you have read this statement and accept these risks.

If you do open Pathscape, any devices secured this way shown as **Read Only**.



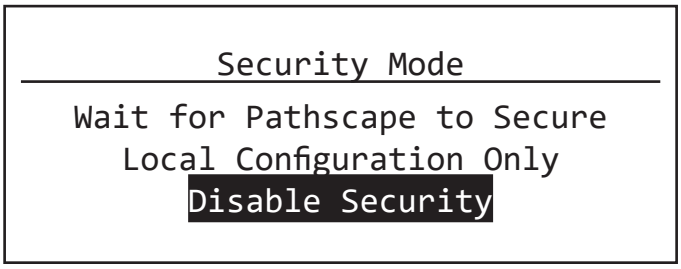
If you want to configure or patch custom universes to this device or use a PC for further configuration, you must use the front panel to **Reset Security** settings, then use Pathscape to add it to a Security Domain.

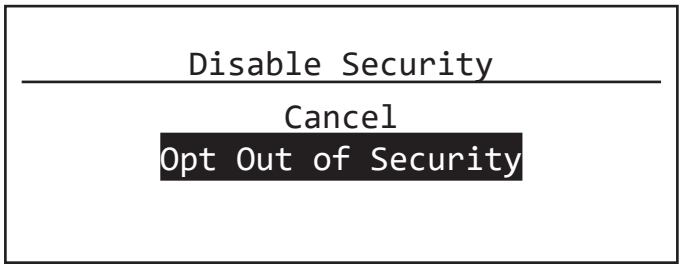
DISABLING SECURITY

With the launch of **firmware version 6.1 for devices with a front panel display and encoder (PWPP RM P8, PWPP RM P4, PWVIA RMs only)**, it is possible to opt out of the security features altogether. This is designed primarily for the rental market where devices may be shipped to various locations for use by different end users, where Domain passwords and Recovery Keys may not be known.

This mode of operation is not a recommended practice. However, if the production is on a dark network with a known crew, risk assessment may be weighed against convenience.

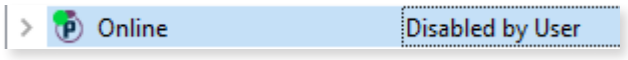
It is only possible to disable security settings from the front panel. **It is not possible to do this from Pathscape. You must perform this action from the Security Mode menu**, which is only shown when no other security mode has been set, i.e. when new from the factory, or after the device has been Factory Defaulted or had its Security Settings reset.





- From the **Security Mode** menu shown on the LCD, turn the encoder to select **Disable Security**. In the submenu, confirm by selecting **Opt Out of Security** again.
- You will then be able to access the menus. The device will appear in Pathscape with the Security Domain shown as "**Disabled by User**".
- On the front panel display, the bottom line will show "`Security: Disabled by User`" as a reminder and warning.

Devices set to **Disabled by User** will behave like legacy devices and are fully Read/Writable by Pathscape **without needing to be logged into a Domain**.



These devices will be fully configurable, resettable and rebootable from any PC that has network access, **including unauthorized parties**.

To re-enable Security on a device that has been **Disabled by User**, use the front panel to Reset Security settings, and add the device to Pathscape as explained above.

PATHWAY ssACN (Secure sACN)

Pathway ssACN (Secure streaming ACN) is a protocol developed by Pathway using much of ANSI E1.31, but adds a layer of authentication. This feature requires **device firmware version 6.0 or later**.

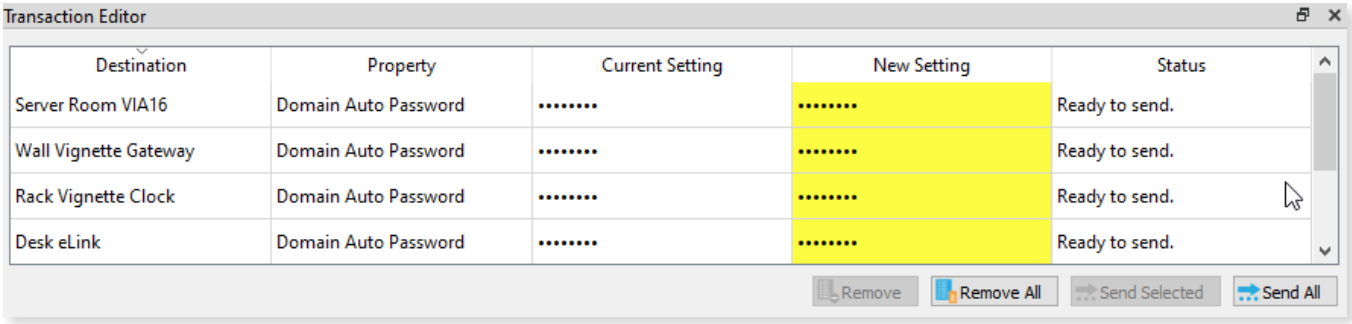
Receiving devices, like Pathport DMX/RDM gateways, share a **secret password** with known controllers in the venue, to verify the data source before driving the lighting rig. A cryptographic hash message is added to each E1.31 packet, verifying the authenticity of the source and the sequence of the data. Any invalid packets are ignored; only the correct lighting data is used during your performances.

If you have disabled security on a device, you will not be offered the ssACN protocol for Tx or Rx.

"Bad actors" cannot spoof a DMX source and send denial-of-service or ransomware attacks as the packets on their unsecured, un-authenticated protocols will be completely ignored by the lighting rig.

DOMAIN AUTO ssACN PASSWORD

When devices are added to a Security Domain, Pathscape generates a secret **Domain Auto ssACN password**, and creates transactions to send this data to each device in the domain. Each Security Domain will have a unique secret Domain Auto password created for it.



NOTE: these transactions will also appear for devices **already** part of a domain, after upgrading those devices to firmware version 6.0 or later.

NOTE that the **Domain Auto** password is **NOT** the same as the **Domain** password. Recall that the Domain password is the the password **you chose** when creating the domain, used for logging in. Pathscape generates the Domain Auto password based on an algorithm. It is **NOT** possible to uncover the "•••••••" and see the value of the password, however all devices on the domain know what it is. This is how the authentication is possible.

CUSTOM ssACN PASSWORD

While in most scenarios the Domain Auto ssACN password will be all that is required, it is possible to specify your own custom ssACN password. See below for details on how to set custom TX (Transmit) and RX (receive) passwords.

This is useful in a few situations:

- **If you need to send DMX data across different Security Domains**: specify a custom **ssACN TX password**, and enter the same password on the receiving devices under **ssACN RX passwords**. The receiving devices will then be able to authenticate that data. Domain Auto passwords, as noted above, are unique per Domain, and will work only with devices on the same domain.
- **If you have a network with multiple consoles**: specify a different TX password for each console, and set the appropriate receiving devices to receive only one password or the other, effectively having them "listen" to traffic from the desired console only.

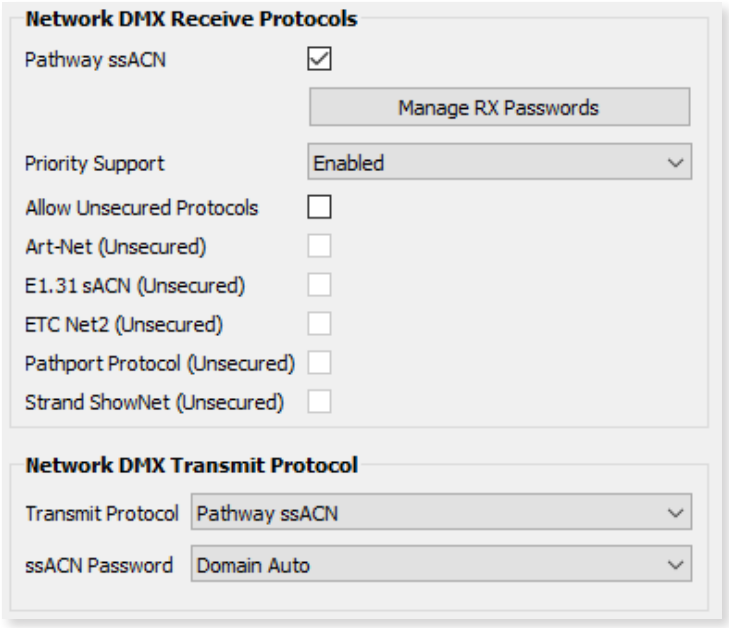
There may be other situations where a custom ssACN password is useful, but we recommend using the Domain Auto password for most systems unless you have unique requirements like the above.

If your console does not support Pathway ssACN and you still want to take advantage of the protocol's security features, consider inserting an eLink between the guest console and your installed network to wrap the generic sACN data for the Security Domain.

CHOOSING PATHWAY ssACN AS NETWORK PROTOCOL

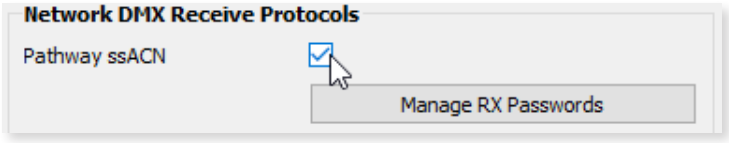
To use Pathway ssACN and ensure the security of the entire network, you must specify all relevant devices to use Pathway ssACN.

In the relevant devices' **base device** properties, there are two sections called **Network DMX Receive Protocols** and **Network DMX Transmit Protocol**.



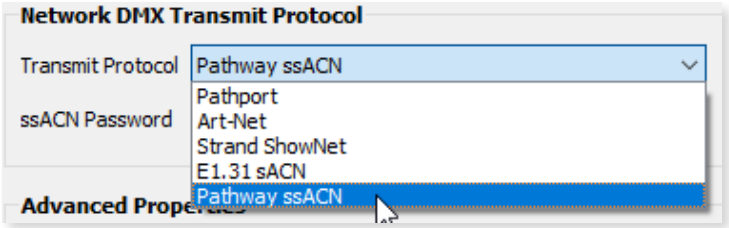
These are the same sections where you would specify your devices to use Network DMX protocols like E1.31 sACN or Art-Net, for example.

In the **Network DMX Receive Protocol** section, simply check the Pathway ssACN checkbox. We recommend unchecking the Allow Unsecured Protocols checkbox, if previously checked, since end devices can receive **both** ssACN and unsecured protocols if left checked.

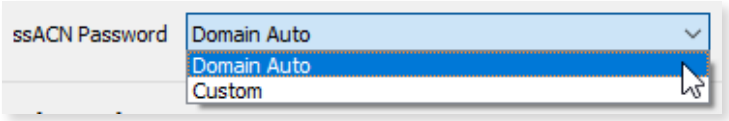


This will ensure the receiving devices will only accept authenticated Pathway ssACN.

In the **Network DMX Transmit Protocol** section, **Pathway ssACN** is simply added to the drop-down menu list of available TX protocols. Choose **Pathway ssACN** from the drop-down menu.

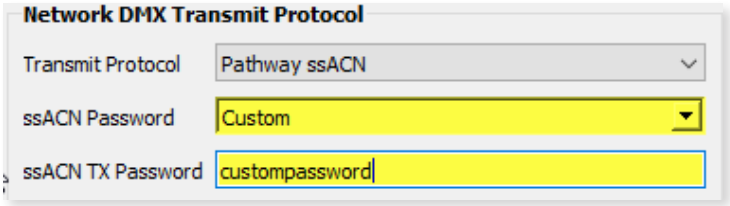


Once you select **Pathway ssACN**, the **ssACN Password** drop-down menu will appear.



Specify here whether the device should use the generated **Domain Auto** password (default), or a custom user-set password.

If you choose **Custom**, the **ssACN TX Password** field will appear.



Enter a custom ssACN TX password for the device here. **NOTE**: this must be done on every device you wish to transmit a custom ssACN password with.

More on managing ssACN Passwords below.

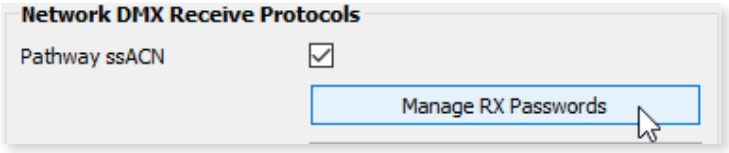
MANAGING PATHWAY ssACN PASSWORDS

In most situations, you will be using the Domain Auto password. In these cases, after configuring your devices to receive and transmit Pathway ssACN, you will not need to do any password management or further configuration.

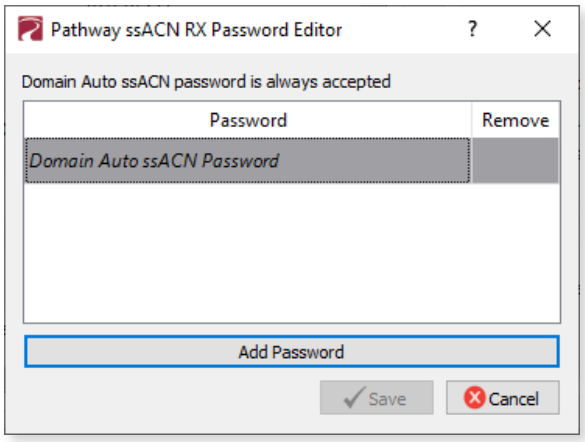
If you are using custom Pathway ssACN passwords, you will need to tell those devices transmitting Pathway ssACN what password to use, as well the devices that are receiving it what passwords to accept.

RX (RECEIVE) PASSWORDS

Under the checkbox for **Pathway ssACN**, there is the **Manage RX Passwords** button.

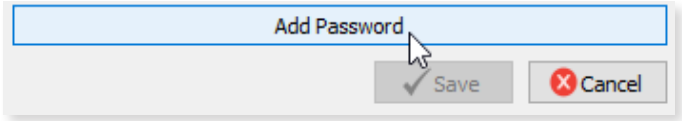


Click it to open the **Pathway ssACN RX Password Editor**.

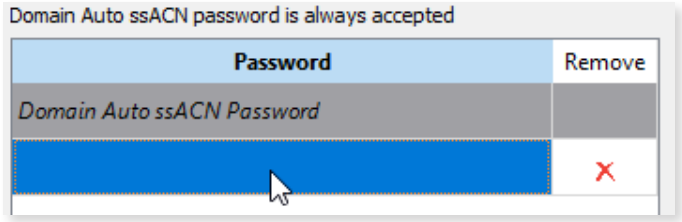


Use the Pathway ssACN RX Password Editor to add custom passwords the selected device should accept.

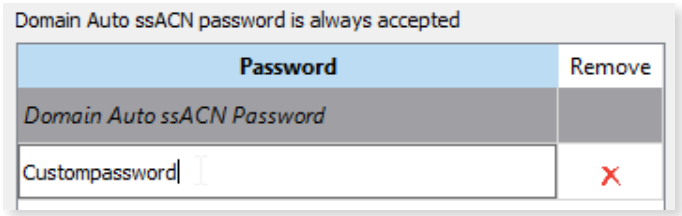
To enter a new password, click the Add Password button.



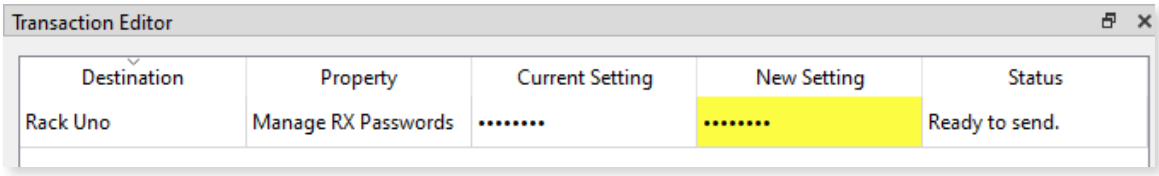
A blank entry will be added to the window.



Double-click on the row and enter your custom password into the text field.



To add additional passwords, repeat the steps above. To delete a password entry, click the ✕ next to the entry you wish to delete. To finish, click the Save button. A transaction will be queued in the Transaction Editor, which must be sent to save changes.



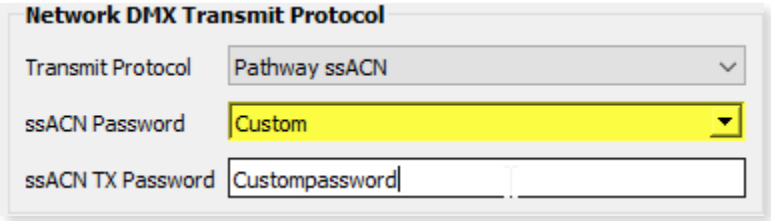
Click the Cancel button to close the window without saving any changes or edits made.

NOTE: the selected device will accept any source transmitting with a password listed in the password editor window. The

Domain Auto password is always accepted.

TX (TRANSMIT) PASSWORDS

Under the **Network DMX Transmit Protocol** , choose Custom under ssACN Password.



The **ssACN TX Password** field will appear. Enter the custom TX password you want this device to use.

NOTES ABOUT PATHWAY ssACN

A device can only have one TX password at a time. You cannot transmit with multiple TX passwords.

However, receive devices, as shown above, can accept any number of different custom passwords.

The **Network DMX Receive Protocol** and **Network DMX Transmit Protocol** properties are set on the base device and apply to all ports or subdevices. You cannot specify different protocols or passwords per port.

SOFTWARE (PATHSCAPE) CONFIGURATION

Wherever possible, we recommend using a PC with Pathscape to configure your PWPP RM P4. For in-depth information on using Pathscape, see the Pathscape manual. Pathscape is available for macOS and Windows from the Pathway website.

If using a PC with Pathscape is not possible or practical, see the section **Front Panel UI and Menu** later in this manual.

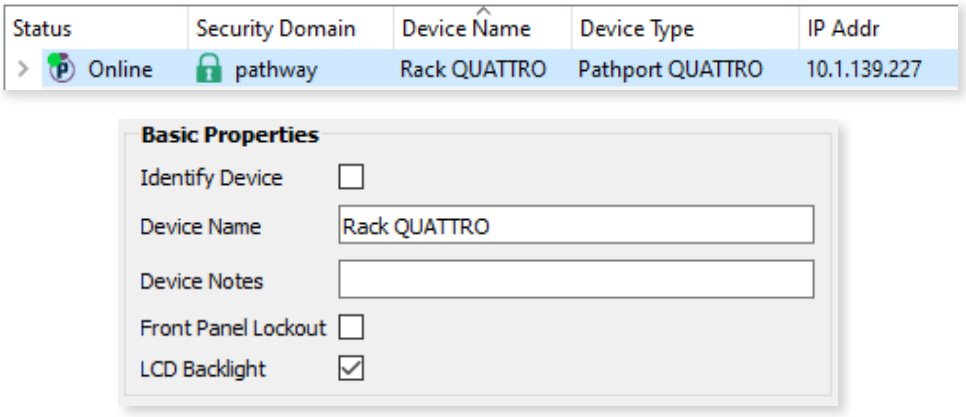
NOTE some features are not available if using only the Front Panel to configure the device.

NETWORK SETUP

PLEASE NOTE: Before any configuration and network setup can be done, including setting the IP, the PWPP RM P4 must be added to a Security Domain. If the device is not added to a Security Domain, it will not be possible to configure any properties.

From the factory, the PWPP RM P4's IP address is static, and set to **10.X.X.X** (where X is between 0 and 254), with a subnet mask of **255.0.0.0** and a default gateway of **10.0.0.1**. Before any additional configuration, set the devices' IP address to the same subnet and IP range as the computer and other devices on the lighting network.

Additionally, the PWPP RM P4's default name in the device list will be shown as its IP address. Give it a useful name before continuing.

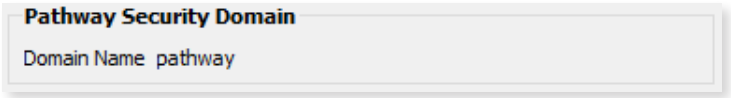


DEVICE PROPERTIES

The following fields are shown in the Device Property Panel in Pathscape. Some are editable, while others are read-only.

NOTE: If all properties are read-only (grayed out and uneditable), make sure you are logged into the correct Security Domain.

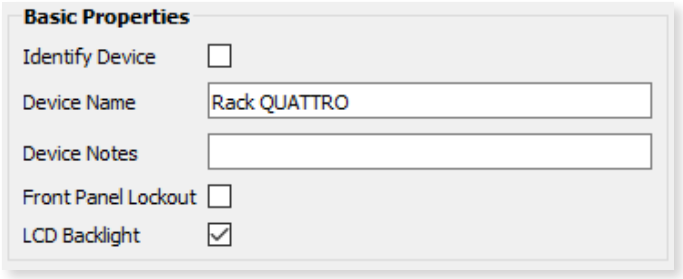
PATHWAY SECURITY DOMAIN



DOMAIN NAME

The name of the Security Domain the device is currently assigned to.

BASIC PROPERTIES



IDENTIFY DEVICE

Checking this box causes device to commence identify behavior (flashing LCD backlight).

DEVICE NAME

A user-configured, soft label for the Gateway. If left blank (and by default) the device name displayed will be the device's IP Address. Shown in the Device window and on Gateway front display.

DEVICE NOTES

A user-configured text description field, shown in the Device view.

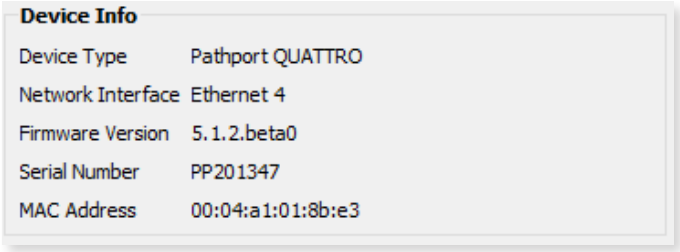
FRONT PANEL LOCKOUT

Checking this will lock the local controls on the front panel of the device. Scrolling menus allow you to read properties, but changing properties is disallowed.

LCD BACKLIGHT

Checking this will enable the LCD backlight on the front panel of the device.

DEVICE INFO



DEVICE TYPE

The device type for the currently selected device.

NETWORK INTERFACE

Shows the name of the NIC (Network Interface Card) the device is communicating to the machine running Pathscape on.

FIRMWARE VERSION

Shows current operating firmware version. See the **Firmware Update** section on how to update the firmware. Read-only.

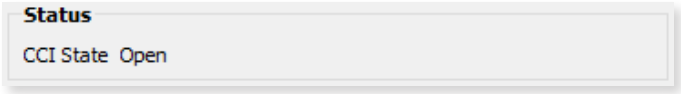
SERIAL NUMBER

Factory-set unique identifier. Read-only.

MAC ADDRESS

Factory-set hardware address. Read-only.

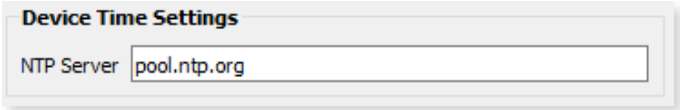
STATUS



CCI STATE

PWPP RM P8 / PWPP RM P4 / PWPP DIN P4 Models. Shows the current state of the Contact Closure Interface (CCI) Input. Values are **Open** (inactive) or **Closed** (active).

DEVICE TIME SETTINGS

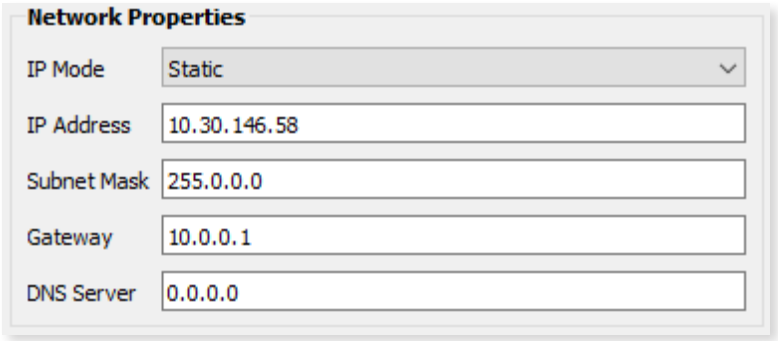


NTP SERVER

PWPP RM P8 / PWPP RM P4 / PWPP DIN P4 Models only. Set the server for NTP (Network Time Protocol). This is to ensure that security certificates are valid, when connecting to SixEye RMM. We recommend using **pool.ntp.org, time.windows.com, time.apple.com** or other publicly available servers**.**

If using the NTP server, ensure that the DNS Server and IP Gateway are set so the device knows how to get to the Internet to find a time server.

NETWORK PROPERTIES



IP ADDRESS

Internet Protocol address (IPv4) of the Gateway.

SUBNET MASK

User-configured subnet mask. Typically, 255.255.255.0 but must be set according to general networking rules.

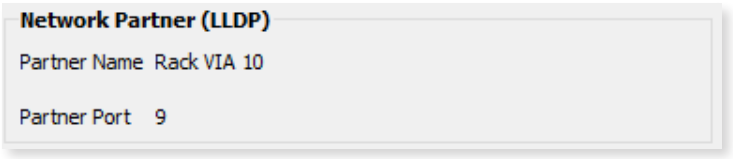
GATEWAY

Specify network gateway address if using **NTP server** and/or **SixEye RMM**.

DNS Server

Hardware-refreshed PWPP RM P8 /PWPP RM P4 /PWPP DIN P4 Models only. Set Domain Name Server for the device here. The DNS should be specified if using and **NTP server** and/or **SixEye RMM**

NETWORK PARTNER (LLDP)



PARTNER NAME

If the upstream switch supports Link Layer Discovery Protocol (LLDP), that device's name will appear here. Read-only.

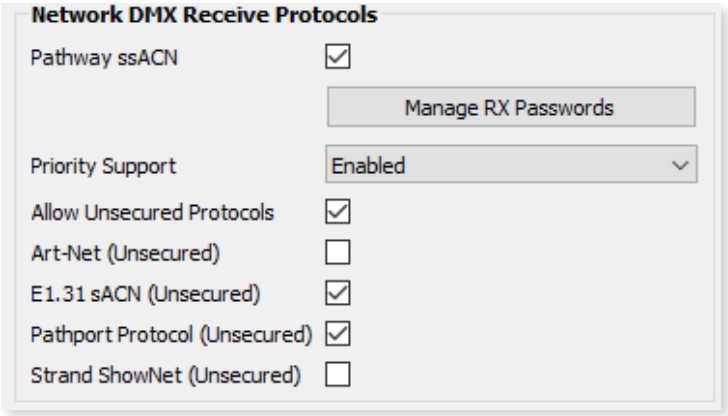
PARTNER MAC

The hardware MAC (Media Access Control) address of the LLDP Partner, if applicable. This property will be hidden if the above Partner Name is displayed, as it is less useful. If the Partner Name is not able to be discover, the Partner MAC will be shown. Read-only.

PARTNER PORT

If the upstream switch supports Link Layer Discovery Protocol (LLDP), the port the current device is connected to will be shown here. Read-only.

NETWORK DMX RECEIVE PROTOCOLS



PATHWAY ssACN

Check this box to enable **Pathway ssACN.**

Click the **Manage RX Passwords** button to configure ssACN Passwords. See the Security section earlier in the manual for details.

PRIORITY SUPPORT

Use the drop-down menu to choose whether the PWPP RM P4 respects the sACN priority (1-200) in the Universe header. Options are **Enabled** (default) or **Disabled**. Applicable to sACN or ssACN only.

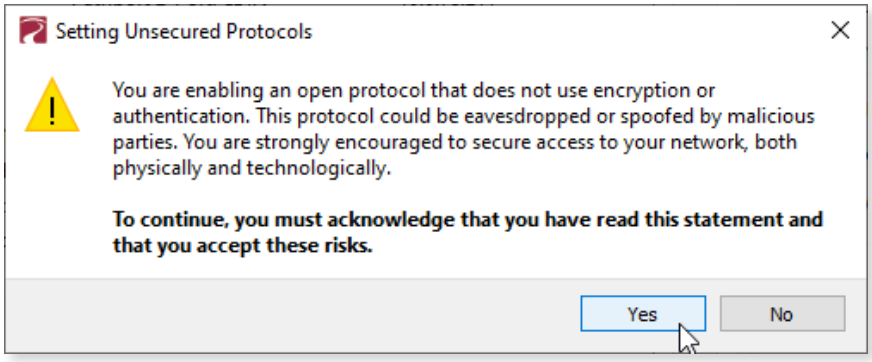
ALLOW UNSECURED PROTOCOLS

Check this box to enable the use of unsecured network protocols (Art-Net, E1.31 sACN, Pathport Protocol, ShowNet). **By default, this property is not enabled**. In order to use the PWPP RM P4 with standard (unsecured) protocols, **this must be enabled**.

WARNING ABOUT UNSECURED PROTOCOLS

You are enabling an open protocol that does not use encryption or authentication. These protocols could be eavesdropped or spoofed by malicious parties. You are strongly encouraged to use Pathway ssACN, and secure access to your network, both physically and technologically. To use unsecured protocols, you must acknowledge that you have read this statement and accept these risks.

After checking this box and sending the transaction, a dialog will appear warning you of the above and asking for confirmation



To continue, you must click the "**Yes**" button to confirm you understand the associated risks.

Art-Net (UNSECURED)

Check this box to enable the receiving of Art-Net. You must check both the **Allow Unsecured Protocols** checkbox and this checkbox to use Art-Net.

E1.31 sACN (UNSECURED)

Check this box to enable the receiving of E1.31 sACN. You must check both the **Allow Unsecured Protocols** checkbox and this checkbox to use standard E1.31 sACN.

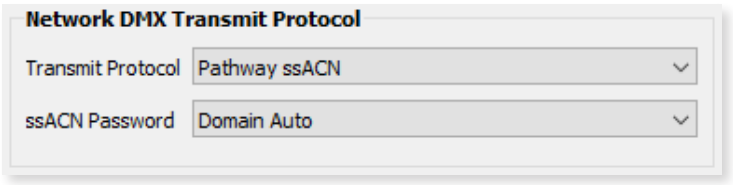
PATHPORT PROTOCOL (UNSECURED)

Check this box to enable the receiving of Art-Net. You must check both the **Allow Unsecured Protocols** checkbox and this checkbox to use Art-Net.

STRAND ShowNet (UNSECURED)

Check this box to enable the receiving of Strand ShowNet. You must check both the **Allow Unsecured Protocols** checkbox and this checkbox to use Strand ShowNet.

NETWORK DMX TRANSMIT PROTOCOL



TRANSMIT PROTOCOL

Use the drop-down menu to select the network protocol the PWPP RM P4 will transmit. Options are:

Pathport will use transmit using unsecured Pathport Protocol.

Art-Net will use transmit using unsecured Art-Net.

Strand ShowNet will use transmit using standard, unsecured E1.31 sACN.

E1.31 sACN will use transmit using standard, unsecured E1.31 sACN.

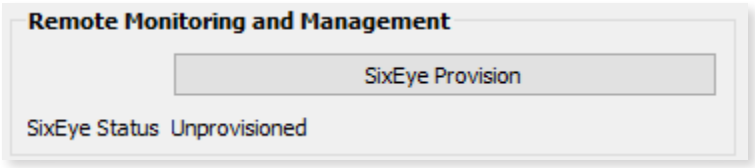
Pathway ssACN will use Pathway's secured sACN for transmitting to the network.

ssACN PASSWORD

Applies only if Pathway ssACN is chosen in the drop-down menu above.

Specifies whether to use the **Domain Auto** or a **Custom** ssACN Transmit password.

REMOTE MONITORING AND MANAGEMENT



For details on how to connect Pathway devices to a SixEye portal, see the **SixEye PROPERTIES** section in the **Pathscape manual**.

SixEye PROVISION

This button will open the SixEye Provision window. In this field, paste the SixEye Device Key and click **Provision**.

SixEye STATUS

This shows the status of the SixEye connection.

Unprovisioned (default).

No Internet Connection. There is a problem with the device finding an Internet connection. Check the device's IP Settings, specifically the Gateway.

DNS Failure. The device has found a connection, but there is a problem with resolving URLs. Check the device's DNS settings.

Invalid System Time. The device has connected to the Internet, but there is a problem with the System Time. Check the device's NTP server settings.

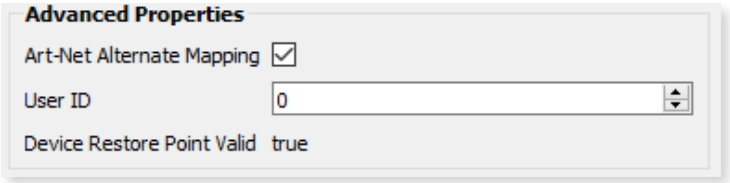
SixEye Init. The device is currently initializing a connection with SixEye.

SixEye Init Error. The device could not initiate a connection with SixEye.

Not Connected. The device is not currently connected to SixEye.

Connected. The device is connected to SixEye.

ADVANCED PROPERTIES



ART-NET ALTERNATE MAPPING

This property will only be visible if Art-Net is enabled under Network DMX Receive Protocols.

Enabled (by default). When enabled, Art-Net Universe 0:0 is treated as Universe 1. When disabled, Art-Net universe 0:0 is ignored.

USER ID

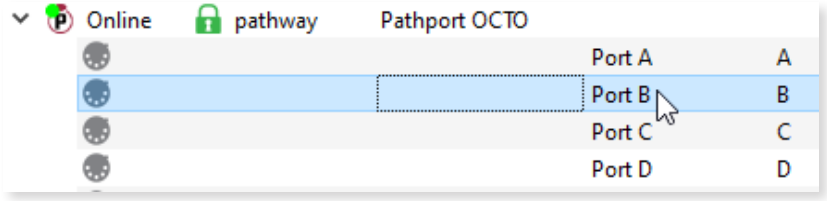
Custom numeric identification for external databases.

DEVICE RESTORE POINT VALID

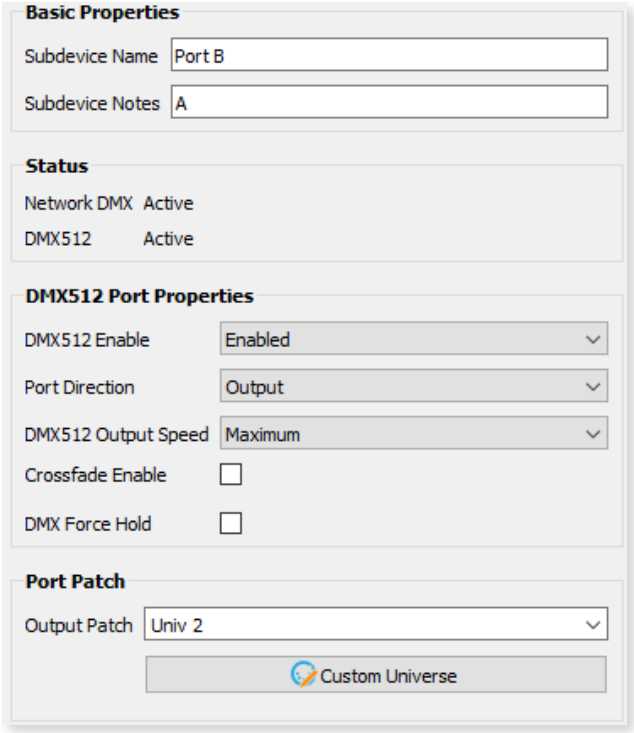
Shows **True** of **False** depending on whether the current Device Restore Point is valid.

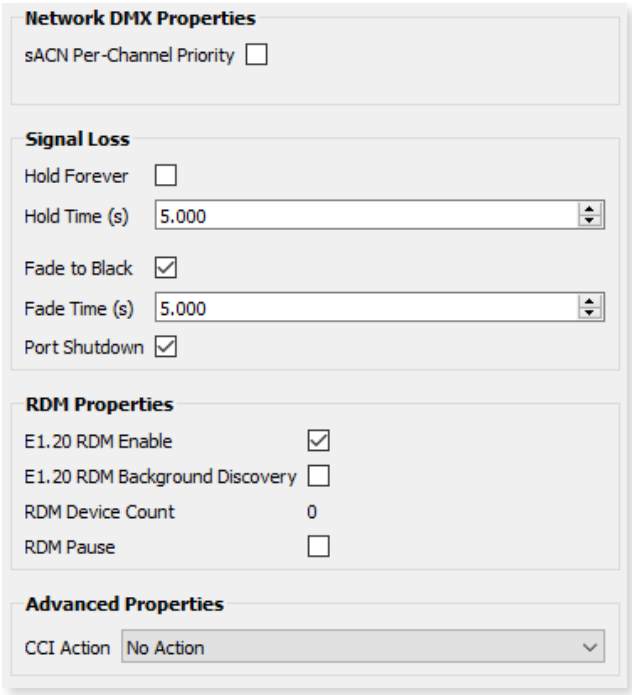
PATHPORT PORT PROPERTIES

Pathport Gateway subdevices are DMX Ports . Gateways have between 1 and 8 ports. Port Direction may be **Input** (receive DMX512 and put Network DMX on network) or **Output** (convert Network DMX from one of the four supported protocols to DMX512). Output ports may also be configured to be RDM controllers. There are two tables of properties based on Port Direction.



OUTPUT PORT PROPERTIES





BASIC PROPERTIES

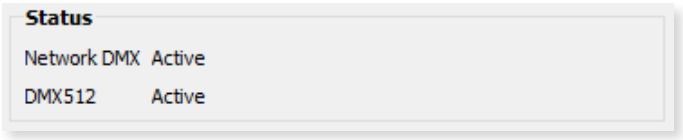
SUBDEVICE NAME

A user-configured, soft label for the Port. By default, based on the number of Ports on a Gateway, the Ports are labeled A through H. It is good practice to label a Port based on where the DMX512 cable is going or its function. (i.e. “Stage Left Boom” or “LEDs in House”).

SUBDEVICE NOTES

A user-configured text description field, shown in the Device window.

STATUS



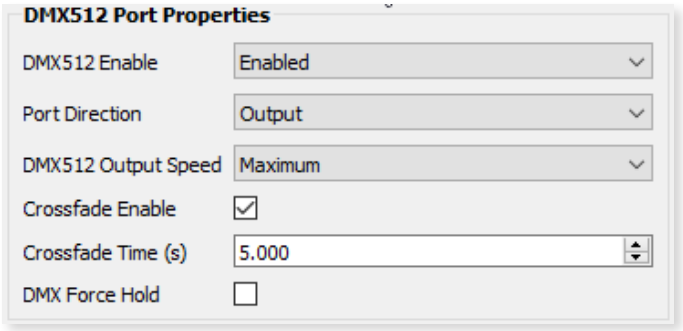
NETWORK DMX

Shows status of the Network DMX source for this Output Port. Will show **Active** when Network DMX stream is present, and **Inactive** if Network DMX stream is lost. Read-only.

DMX512

Shows activity of the hard DMX512 Port. Will show **Active** when actively transmitting DMX512, and **Inactive** when it is not. Read-only.

DMX512 PORT PROPERTIES



DMX512 ENABLE

For debugging purposes or otherwise, you may want to disable a DMX port. All other properties will remain unchanged. Apart from the fact that the line is still terminated, this is electrically equivalent to unplugging the DMX512 cable.

Use the drop-down menu to select **Enabled** or **Disabled**.

PORT DIRECTION

Input or **Output**. This table shows the properties of an **Output** port.

DMX512 OUTPUT SPEED

ANSI E1.11 compliant devices should be able to receive at Maximum speed (42 Hz), but some devices may require you to lower the number of DMX512 packets per second. The slowest rate is 30 Hz. Values are **Maximum**, **Fast**, **Medium** and **Slow**.

CROSSFADE ENABLE

If a Priority changes either as defined by the Pathscape DMX Patch Priorities or the E1.31 sACN Priority, the Gateway will fade rather than snap to the new levels. The last frame of the old source is frozen during the fade.

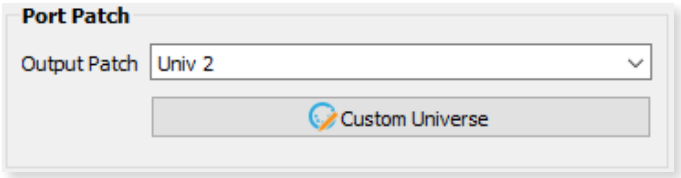
CROSSFADE time (s)

Sets the crossfade time, as defined above in **Crossfade Enable**.

DMX FORCE HOLD

Check this box to force the DMX512 port to snapshot the current DMX levels and maintain them indefinitely, ignoring any further changes. Useful to lock out any unintended changes once levels are set as desired.

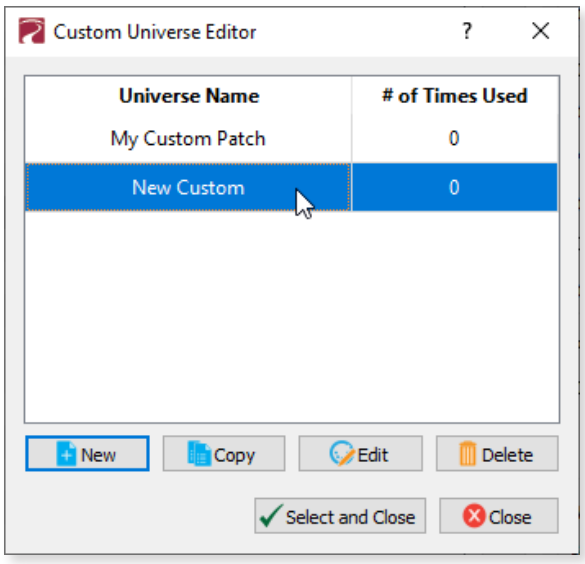
PORT PATCH



OUTPUT PATCH

Use the drop-down menu to select the output patch for the port. By **default**, the drop-down menu lists standard Universes 1-16, and Custom patches, even if not in use. To patch the port to a new standard Universe not in the list, simply type the Universe number into the field.

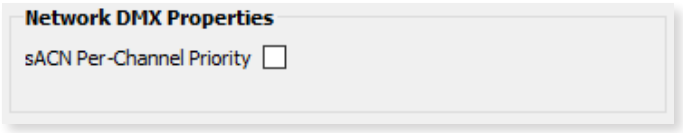
Click the **Custom Universe** button to open the Custom Universe Editor.



The **Custom Universe Editor** window is a quick way to **Add New Custom Universes**, and **Copy**, **Edit** or **Delete** existing ones, just like in the **DMX Patch** tab. Pathscape also will show **how many times** each Custom Patch is being used.

Select a Custom Patch name and click the Select and Close to set the port to that patch. Click the Close button to discard changes.

NETWORK DMX PROPERTIES

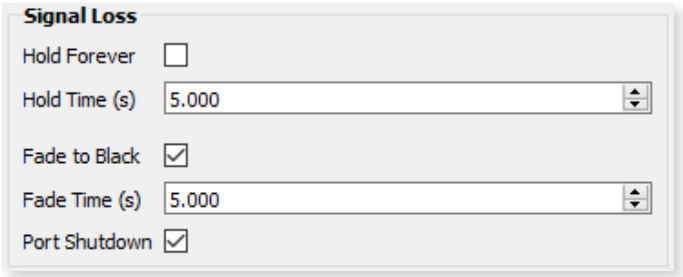


sACN PER-CHANNEL PRIORITY

In the base Gateway device's **Network DMX Receive Protocols**, there is a property **Priority Support** which determines if the Gateway respects the priority (1-200) in the Universe header. This property extends that to each slot in the universe. It is off by default.

Check this box to **enable** per-channel priority.

SIGNAL LOSS



HOLD FOREVER

If enabled, Signal Loss **Hold Time**, Signal Loss **Fade to Black** and Signal Loss **Port Shutdown** are ignored. The DMX Output Port will continue outputting the last received packet indefinitely in the event of Network DMX signal loss.

HOLD TIME (s)

If Signal Loss **Fade to Black** or Signal Loss **Port Shutdown** is enabled, the port will continue outputting the last packet it received until this time has expired.

FADE TO BLACK

If the Network DMX stream ceases, all 512 slots of the DMX512 will fade to a value of 0%.

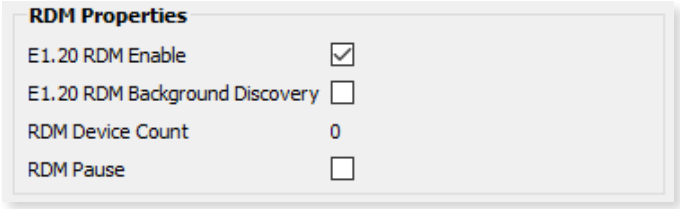
FADE TIME (s)

Applicable when **Fade to Black** is enabled. Defines the time over which the Fade to Black above will take place.

PORT SHUTDOWN

If the Network DMX stream ceases and Hold Forever is not enabled and the Fade Time has expired, the port will "turn off". Apart from the fact that the line is still terminated, this is electrically equivalent to unplugging the DMX512 cable. This is **enabled** by default.

RDM PROPERTIES



Pathscape is a very powerful RDM controller that allows you to identify RDM devices and set properties like mode and starting address.

E1.20 RDM ENABLE

Enabled (Default).

When disabled, no Alternate Start Code packets will be sent on the DMX512 link. Non-RDM compliant devices may react badly to RDM packets.

E1.20 RDM BACKGROUND DISCOVERY

Depending on the number of RDM devices on this port, discovery can take anywhere from a second to several minutes. Turning **on** Background Discovery allows the Gateway to keep an up-to-date list of which devices are online vs. offline.

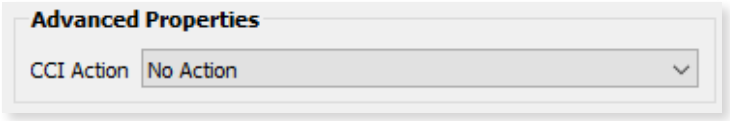
RDM DEVICE COUNT

This will show the number of RDM devices detected on the selected DMX Port. Read-only.

RDM PAUSE

Check this box to suspend all RDM discovery (quick or background), RDM GET and SET commands. Useful in a show-mode setting where RDM could negatively impact network performance.

ADVANCED PROPERTIES



CCI ACTION

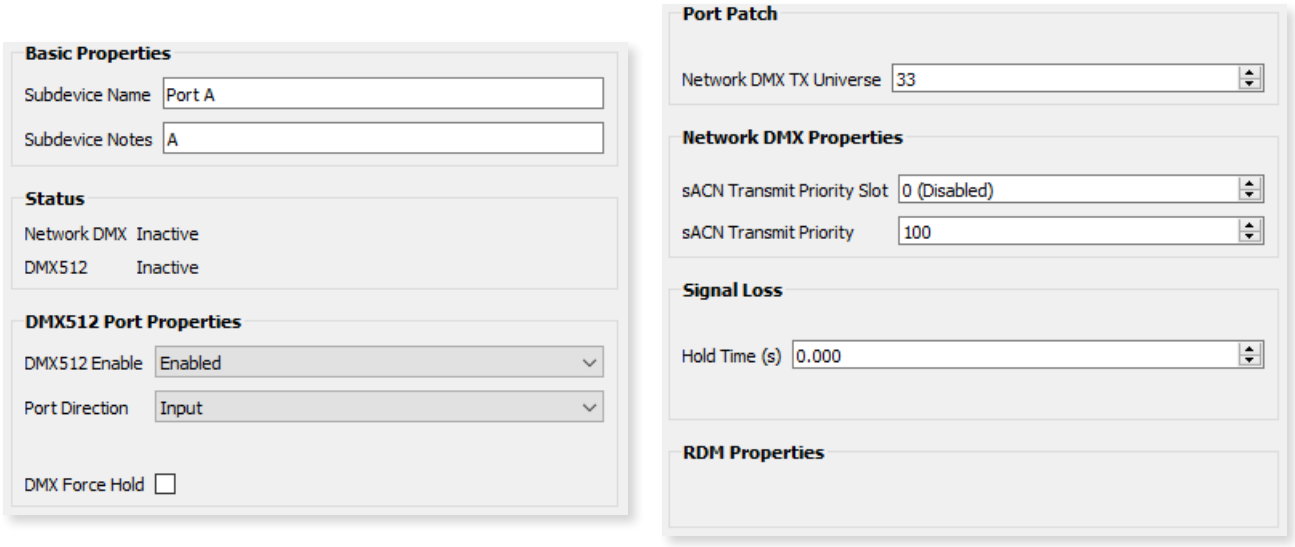
Hardware-refreshed PWPP RM P8/PWPP RM P4/PWPP DIN P4 Models only. Choose the function of the CCI input, if desired. When the Contact Closure Interface is **closed** (activated), the chosen action will be performed on the selected port.

No Action: No action is taken.

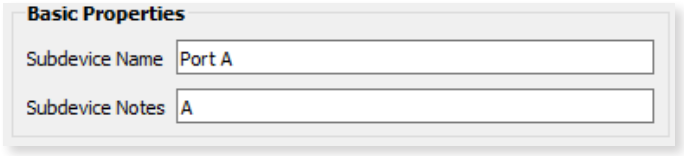
DMX Force Hold: Activates DMX Force Hold on the specified port, as described above. When the CCI input is opened, the DMX Force Hold will be deactivated.

RDM Pause: Activates RDM Pause on the specified port, as described above. No effect if used on an Input port.

INPUT PORT PROPERTIES



BASIC PROPERTIES



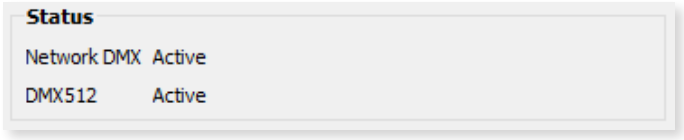
SUBDEVICE NAME

A user-configured, soft label for the port. By default, based on the number of ports on a gateway, the ports are labeled A through H. It is good practice to label a port based on where the DMX512 cable is coming from. (i.e. “Console Port 3” or “House Lights”).

SUBDEVICE NOTES

A user-configured text description field, shown in the Device window.

STATUS



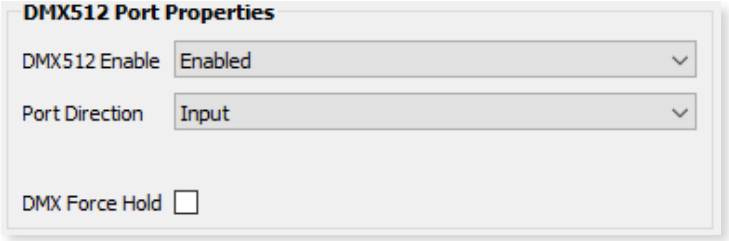
NETWORK DMX

Shows status of the Network DMX source for this Input Port. Will show **Active** when Network DMX stream is present, and **Inactive** if Network DMX stream is lost. Read-only.

DMX512

When **Active**, there is a valid source of DMX512 coming into the Gateway. Read-only.

DMX512 PORT PROPERTIES



DMX512 ENABLE

For debugging purposes or otherwise, you may want to disable a DMX port. All other properties will remain unchanged. Apart from the fact that the line is still terminated, this is electrically equivalent to unplugging the DMX512 cable.

Use the drop-down menu to select **Enabled** or **Disabled**.

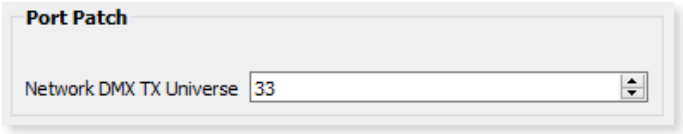
PORT DIRECTION

Input or **Output**. This table shows the properties of an **Input** port.

DMX FORCE HOLD

Check this box to force the DMX512 port to snapshot the current DMX levels and maintain them indefinitely, ignoring any further changes. Useful to lock out any unintended changes once levels are set as desired.

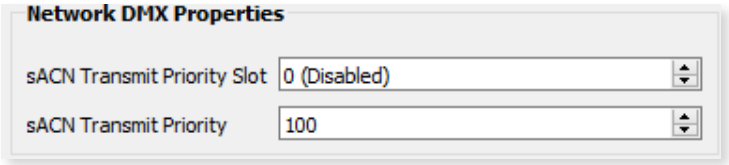
PORT PATCH



NETWORK DMX TX UNIVERSE

Specify the Network DMX Universe on which to transmit the DMX512 input.

NETWORK DMX PROPERTIES



sACN TRANSMIT PRIORITY SLOT

You can allocate one of the 512 slots of the output patch to set the Transmit Priority as described below. Any value of d200 (about 78%) is converted to a priority of 200. Zero values are converted to priority 1, the lowest priority in E1.31.

sACN TRANSMIT PRIORITY

When E1.31 sACN or Pathway ssACN is put on the network, it will be tagged with a priority level. At output ports, multiple sources will HTP levels if their priorities match, otherwise they will arbitrate. The default TX priority per Port is 100. Valid priorities are between 1 and 200 where 200 is the highest priority possible.

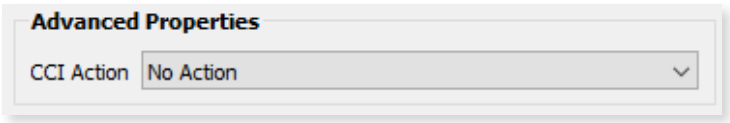
This property is only visible if the above property **sACN Transmit Priority Slot** is set to 0 (disabled)

SIGNAL LOSS

HOLD TIME (s)

If the DMX512 source ceases, the Network DMX will continue to be refreshed to the network using the levels from the last packet the gateway received until this timer expires.

ADVANCED PROPERTIES



CCI ACTION

Hardware-refreshed PWPP RM P8/PWPP RM P4/PWPP DIN P4 Models only. Choose the function of the CCI input, if desired. When the Contact Closure Interface is **closed** (activated), the chosen action will be performed on the selected port.

No Action: No action is taken.

DMX Force Hold: Activates DMX Force Hold on the specified port, as described above. When the CCI input is opened, the DMX Force Hold will be deactivated.

RDM Pause: Activates RDM Pause on the specified port, as described above. No effect if used on an Input port.

PATCHING PORTS

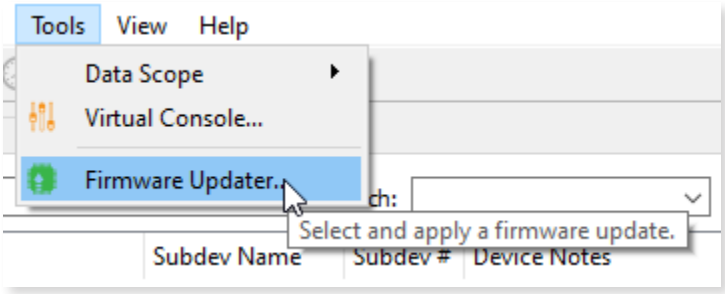
For in-depth instructions on patching the ports on your PWPP RM P4, refer to the **Pathscape manual** section titled **DMX Patch**.

UPGRADING DEVICE FIRMWARE

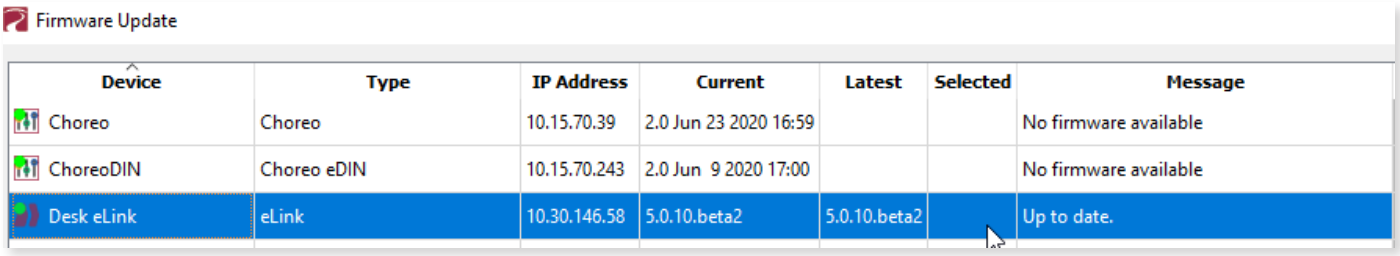
Firmware upgrades may only be done using Pathscape.

The most recently released firmware is bundled with the most recent version of Pathscape. To ensure you have the most up-to-date firmware available for upgrading, ensure you have downloaded the most recent version of Pathscape from the Pathway site, https://www.pathwayconnect.com.

To upgrade a device, ensure the device's IP address is configured correctly and is on the same subnet and IP range as the computer. Open Pathscape, click the Tools menu, and select the **Firmware Updater...** menu item.



This will bring up the Firmware Update window.



Select the device(s) you want to upgrade and click the Select Latest button at the bottom of the window. The latest firmware version will be shown in the table next to "**Current**". Click the Send Firmware button and wait for the progress bar(s) to finish. After the device(s) reboot, the firmware will be updated.

WARNING: **Be careful when updating firmware on multiple devices at once.**

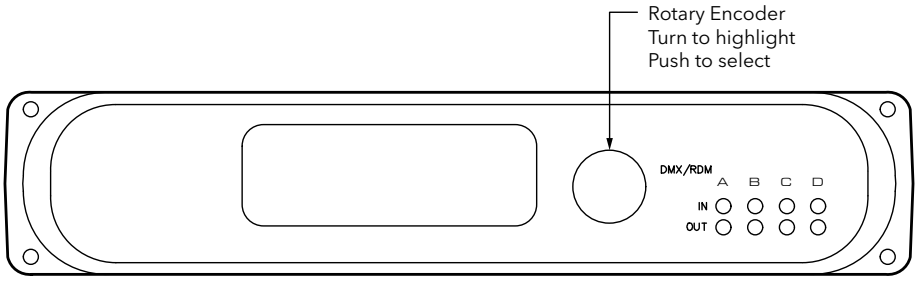
It is strongly recommended that you do not update PWVIA Switches and connected PoE devices at the same time. It is possible for the firmware update process to reboot the Switch before the data has finished writing to the PoE devices' memory. If the PWVIA Switch reboots at this point, the connected PoE devices' power will be cut off, and could be rendered inoperable, in a "bricked" state.

It is advised to update the Switch first, wait for it to reboot, and then update the connected PoE devices, or vice versa.

FACTORY DEFAULT

In the event of a loss of communication with the device, it is possible to reset the switch to factory settings.

To factory default the PWPP RM P4, turn the encoder knob to the main menu, which is the default menu showing the switch's name and IP address. Click in the encoder to access the main menu.




```
Base Configuration
Network Setup
Device Info/Status
Protocol Support
Admin/Security
<Back>
```

Scroll the encoder knob until "**Admin/Security"** is highlighted, and click in the knob. Under the Admin/Security menu, scroll down to "**Factory Default**", and click in the knob.

```
Admin/Security
Factory Default
Manage Restore Point
Reset Security
Reboot
<Back>
```

This will show the Factory Default menu. Here you have several options.

```
Factory Default
Keep Net Setup & Restore Pt.
Keep Restore Point
Wipe All Configuration
<Back>
```

If you choose **Wipe All Configuration** it will completely restore the device to the same state as it left the factory. This will erase any Device Restore Point saved on the unit.

You can also choose **Keep Restore Point** to preserve any saved Restore Point, but be aware that the restore point could have saved properties that are the cause of the communication loss, and recalling that restore point could cause the same issues.

The device will then reboot, having reset itself to the Factory settings. Before configuration can be restored, the unit's Security Mode must be configured (add to a Security Domain, enable Local Configuration Mode, or Disable Security).

FRONT PANEL LOCKOUT

If the device has **Front Panel Lockout** enabled, you will not be able to make changes from the front panel. To address this, there is a 30-second delay before the LCD Lockout takes effect, after the PWPP RM P4 boots up.

First, hard reboot the device (either unplug and re-plug the DC power source, or power cycle the PoE source, as applicable), and then **within 30 seconds** after the switch has booted up, perform the above action. After 30 seconds, the front panel UI will be locked out again.

FRONT PANEL UI AND MENU

The PWPP RM P4 features a front panel UI, consisting of an LCD and a rotary pushbutton encoder for navigating menus and selecting options. If it is not possible to use a PC with Pathscape, you may use the front panel.

NOTE All the menu items reflect device properties in Pathscape. For more detail on a particular menu item, see the above sections that explain each property in more detail.

BEFORE YOU START

Some options and functionality on the device will be unavailable if configuring the device using only the front panel. We **highly** recommend using Pathscape.

You will need to choose a **Security Mode** before you are able to configure the device (see next section).

If set to **Local Configuration Only** (Read-only) mode or the security features are **Disabled**, some functionality will not be available such as Pathway ssACN. Pathway ssACN needs the device to be part of a Security Domain in order to authenticate and send traffic on that protocol.

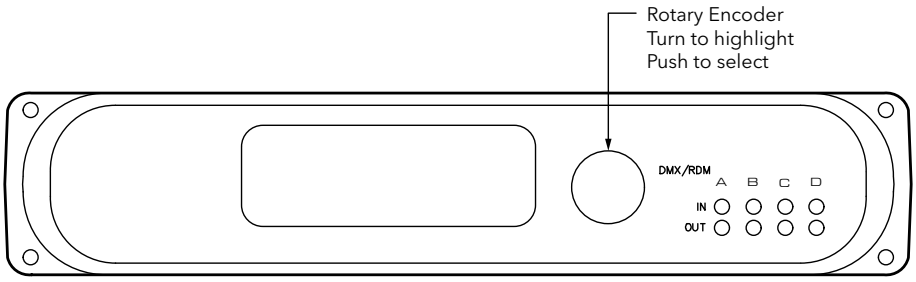
Non-standard Universes (Custom Patches) can only be edited and assigned to Ports using Pathscape.

If you must use the device without Pathscape, you must either set it to **Local Configuration Only** or **Opt Out (Disable) security features (not recommended)** and use **Unsecured** protocols only.

WARNING ABOUT UNSECURED PROTOCOLS

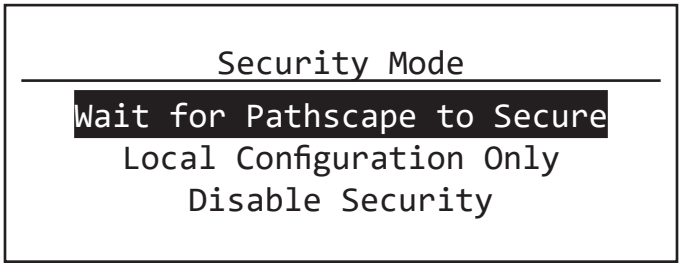
You are enabling an open protocol that does not use encryption or authentication. These protocols could be eavesdropped or spoofed by malicious parties. You are strongly encouraged to use Pathway ssACN, and secure access to your network, both physically and technologically. To use unsecured protocols, you must acknowledge that you have read this statement and accept these risks.

FRONT PANEL UI



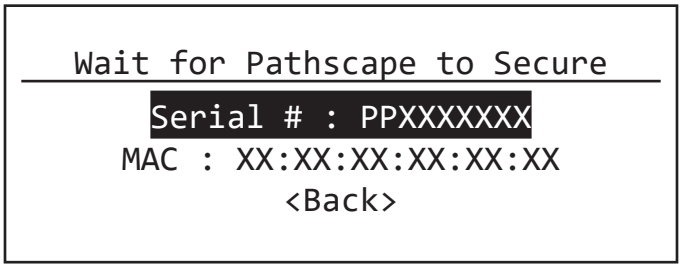
SETTING SECURITY MODE

When the device boots up for the first time, or if it has been Factory Defaulted or had its Security Settings reset, the Security Mode screen will be shown.

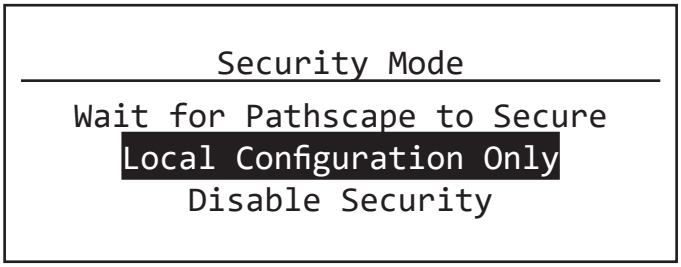


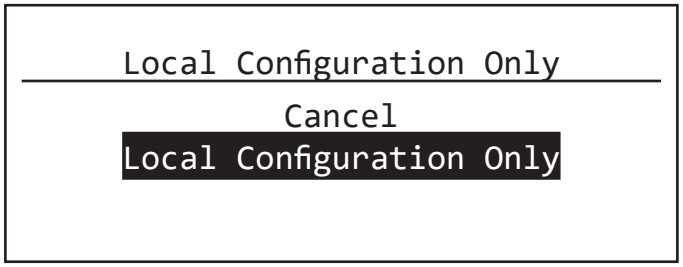
Before you can configure and use the device, you must either:

- **Use Pathscape to Secure the device** (Add it to a Security Domain). **No input from the front panel is required here**. Clicking the encoder knob to select **Wait for Pathscape to Secure** will show the device Serial Number and MAC Address, in cases where this may be helpful for device identification



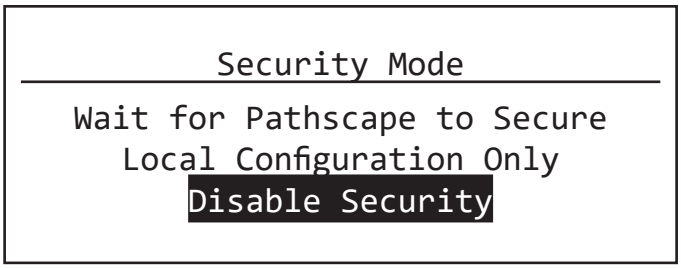
- Enable **Local Configuration Only** (Read only) mode. Turn the encoder to select **Local Configuration Only**. In the submenu, confirm by selecting **Local Configuration Only** again. You will then have full access to the menus.

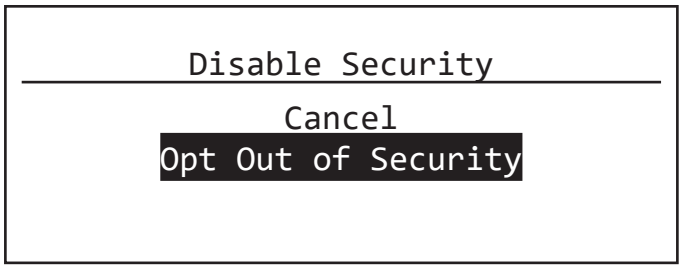




In Local Configuration / Read Only mode, **Pathway ssACN** (Secure sACN) is not available. To use other standard (unsecured) protocols, you **must manually enable them** (see below). As explained above, you cannot use Pathscape to configure the device in this mode.

- **Disable (Opt out of) Security features** altogether. **This mode of operation is not a recommended practice**. However, if the production is on a dark network with a known crew, risk assessment may be weighed against convenience.



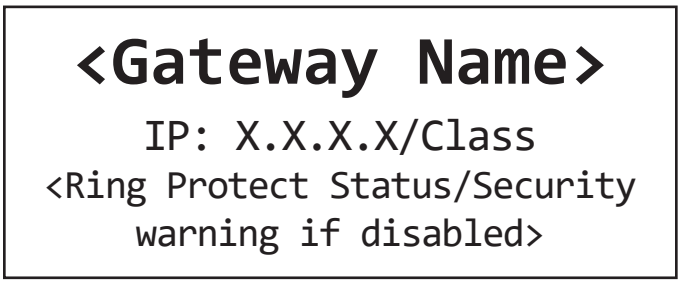


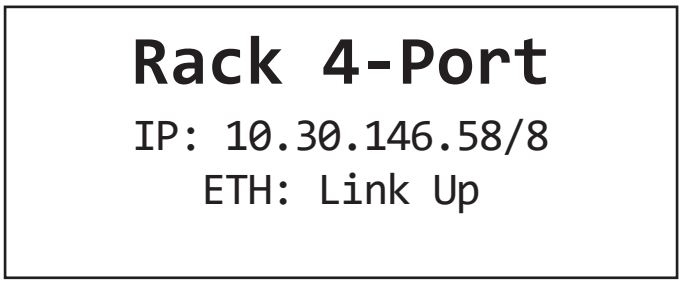
- From the **Security Mode** menu shown on the LCD, turn the encoder to select **Disable Security**. In the submenu, confirm by selecting **Opt Out of Security** again.
- You will then be able to access the menus. The device will appear in Pathscape with the Security Domain shown as "**Disabled by User**". It will behave like a legacy device; all properties will be Read/Writable.
- On the front panel display, the bottom line will show "`Security: Disabled by User`" as a reminder and warning.

MAIN DISPLAY MESSAGES

When idle, the main LCD will show the device soft label (Name) and its IP address. When the device has an active network connection, "`ETH: Link Up`" will be shown at the bottom of the LCD. If the device does not have a network connection, "`ETH: Link Down`" will be shown.

If the switch has been set to Disable security features, it will show "`Security: Disabled by User`" as a reminder and warning.



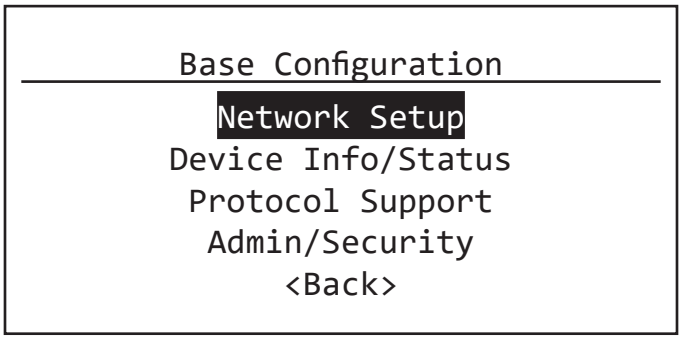


The gateway name will be that soft label given to the device in Pathscape. If no soft label has been assigned to the gateway, its IP address will be shown as its name in the top line, in addition to the middle line.

The subnet class, shown after the IP address on the middle line, will be "/8", "/16" or "/24". These are respectively, Class A subnet mask of 255.0.0.0, a Class B subnet mask of 255.255.0.00, and a Class C subnet mask of 255.255.255.0.

USING THE FRONT PANEL UI

With the main screen (above) showing on the LCD, press in the encoder knob. The base configuration menu will be shown.



Turn the knob to scroll up or down the menu. The currently selected menu item is shown in White on Black. Push the knob to enter sub-menus. Top-level menu entries are shown above.

For all menus and submenus, the current selection will be highlighted in White on Black. Push the encoder knob to reach further options, or to select the currently selected item. If choosing from a list of options, the **currently enabled** value will be shown with asterisks on either side of it, e.g. ***Current Property Value***.

Some menus, such as **Network Settings**, require the user to scroll down to **accept** or **discard** any changes made. The **<Back>** option will always move the menu up one level. The current menu will time out after approximately 30 seconds.

FRONT PANEL LOCKOUT

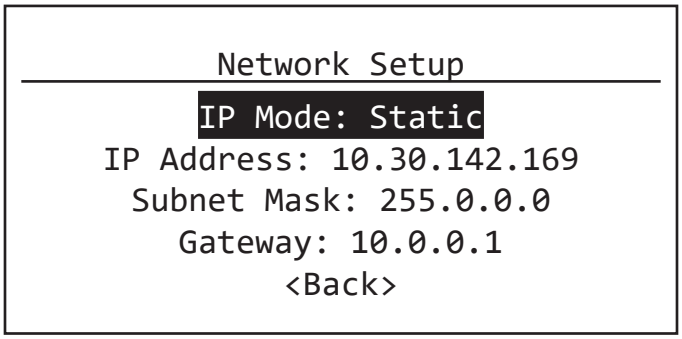
If using Pathscape, it is possible to enable the option **Front Panel Lockout**, which disables the ability to make any changes to the device from the front panel UI. You can still navigate the menus to review settings, but cannot change any properties.

The Front Panel Lockout is temporarily disabled for 30 seconds after the device boots up. This window allows for changes to be made when a Pathscape connection is not available.

NOTE: It is not possible to disable the Front Panel Lockout from the front panel itself; it must be done from Pathscape.

MENUS

NETWORK SETUP



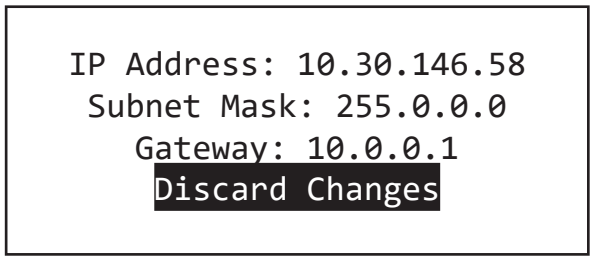
This menu allows review and changes to the device IP mode, IP address, subnet mask, and default gateway. Scroll the encoder knob to highlight the property you want to edit, and push the knob to edit the value. Scroll the knob again to choose the new value, and push the knob to confirm.

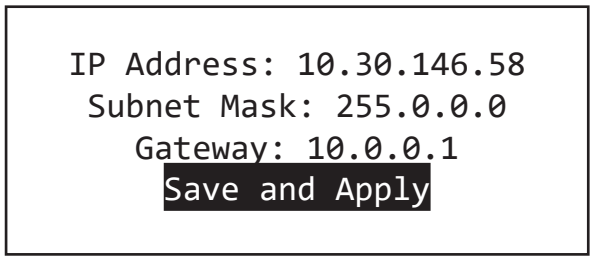
Depending on the item you are editing, you may have to scroll down to select the **<Back>** option to return to the previous menu, or select **Save and Apply** to confirm. In some menus you may also select **Discard Changes** to return to the previous menu without committing changes.

Menu Item	Description
IP Mode	Determines how the device's IP settings will be obtained. **Static (default)**: IP Settings manually set by user. **Dynamic**: IP Settings will be obtained from a DHCP server. **<Back>**: Return to previous menu
IP Address	Manually sets IP address (IPv4). Turn encoder to set each octet. Push to accept and move to next octet. Illegal values are not accepted.
Subnet Mask	Set subnet mask for the device. Only valid masks are shown. Turn knob to select from list of valid masks.
Gateway	Set default gateway for the device. Only valid gateways are accepted. Turn knob to set each octet. Push to accept. You will only be able to edit the octets appropriate based on your Subnet Mask. Gateways will need to be set for access to the Internet for SixEye Cloud Management.
<Back>	Return to previous menu.

NOTE: When IP Mode is set to "Dynamic", it is still possible to manually adjust the IP settings. This practice is not recommended as the changes will not stick.

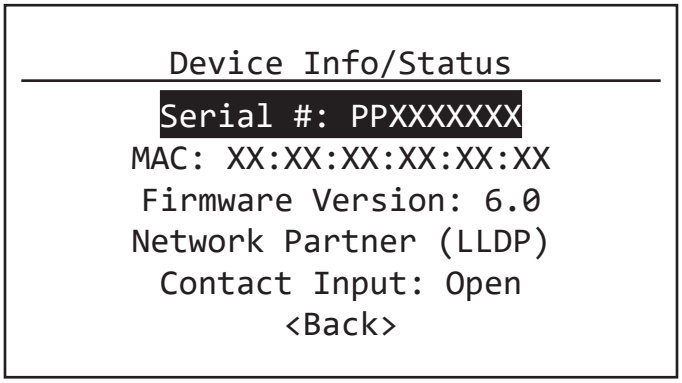
Once the values have been set, acceptance options appear on the bottom line of the screen. By default, **Discard Changes** will be highlighted. Click the knob to cancel and return to previous menu. Turn the knob to select **Save and Apply** to save changes and return to the **Network Setup** menu.





DEVICE INFO/STATUS

This menu allows review of several device properties. These are read-only.

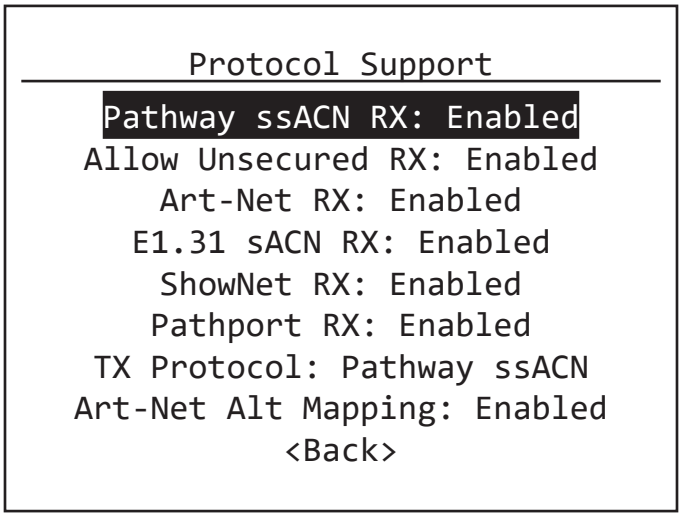


Menu Item	Description
Serial #	Factory-assigned, Pathway serial number. Read-only.
MAC	Factory-assigned media access control (MAC) address. Read-only.
Firmware Version	Current operating firmware version. Firmware may be updated using Pathscape. Read-only.

Menu Item	Description
Network Partner (LLDP)	Opens a sub-menu showing the Network LLDP Partner information, if applicable. Name: Shows the name of the LLDP Partner, if found. IP Address: Shows the IP address of the LLDP Partner. Subnet Mask: Shows the subnet mask of the LLDP Partner. Gateway: Shows the default gateway for the LLDP Partner. The following rows will show information about the LLDP Partner device, if they can be retrieved, including: Manufacturer Model number or name Device serial number Device firmware version Device MAC address <Back>: Returns to previous menu.
Contact Input	Shows the status of the Contact Closure Input (CCI). Values are **Open** (inactive) or **Closed** (active).
<Back>	Return to previous menu.

PROTOCOL SUPPORT

This menu contains settings and sub-menus pertaining to Network DMX Receive and Transmit protocol selection and Art-Net Alternate Mapping.

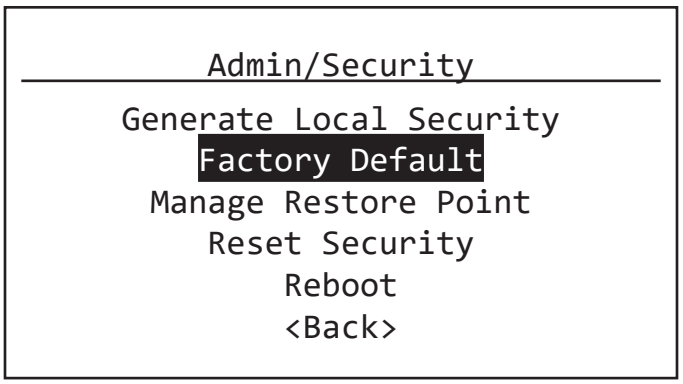


The above menu is laid out in a manner that reflects the property locations in the Pathscape Properties pane as close as possible. Note that some property names are shortened in order to fit on the LCD screen.

Menu Item	Description
Pathway ssACN RX:	**Enable** (default) or **Disable** receiving of Pathway ssACN.
Allow Unsecured RX	**Enable** or **Disable** (default) the receiving of unsecured Network DMX Protocols.
Art-Net RX	**Enable** or **Disable** (default) the receiving of Art-Net. If **Allow Unsecured RX** is set to Disabled, this menu item will be hidden.
E1.31 sACN RX	**Enable** or **Disable** (default) the receiving of E1.31 sACN. If **Allow Unsecured RX** is Disabled, this menu item will be hidden.
ShowNet RX	**Enable** or **Disable** (default) the receiving of Strand ShowNet. If **Allow Unsecured RX** is Disabled, this menu item will be hidden.
Pathport RX	**Enable** or **Disable** (default) the receiving of Pathport Protocol. If **Allow Unsecured RX** is Disabled, this menu item will be hidden.
TX Protocol	Select the Network DMX protocol the PWPP RM P4 should use when transmitting. Options are: **Pathport**: Use Pathway Pathport protocol **Art-Net**: Use Art-Net protocol **ShowNet**: Use Strand ShowNet protocol **E1.31sACN**: Use standard E1.31 sACN protocol **Pathway ssACN** (default): Use Pathway ssACN protocol <Back>: Return to previous menu.
Art-Net Alt Mapping	When enabled, Art-Net Universe 0:0 is treated as Universe 1. When disabled, Art-Net universe 0:0 is ignored and Art-Net Universe 1 is the same as Pathscape Universe 1. Select whether Art-Net Alternate Mapping is **enabled** (default) or **disabled**.
<Back>	Return to previous menu.

ADMIN/SECURITY

This menu contains settings and sub-menus pertaining to rebooting or factory defaulting the device, creating or recalling device restore points, or generating or resetting security settings.

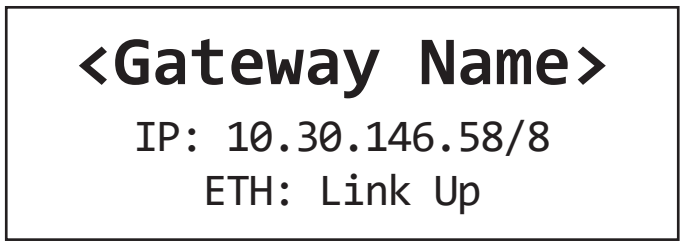


Menu Item	Description
Generate Local Security	**Will appear only when device is not secured,** e.g. when powered on for the first time, or after being factory defaulted or after having security settings reset. Selecting this will generate local security for the device. You will be able configure the device using the front panel **only**; you will **not** be able to change settings using Pathscape. Additionally, some functionality will be **unavailable** (i.e. Pathway ssACN and Custom Patches). To enable Pathway ssACN and configuration using Pathscape, the device must be added to a Security Domain. If already Locally Secured, you must factory default the device or reset its security settings, then use Pathscape to add it to a Security Domain. See the Security section earlier in the manual for detailed instructions. Once the device is secured (whether by Local Security or a Security Domain) this menu item will not be shown.
Factory Default	Allows you to restore the device to its factory settings, with a few options. You may choose to: **Keep Net Setup & Restore Pt.**: Resets all device settings except current network settings and any saved restore point. **Keep Restore Point**: Resets all device settings, including network settings, but keeps any saved restore point. **Wipe All Configuration**: Resets all device settings, including all network settings, security settings and deletes any restore point. For each option, you will have to confirm your decision to factory default the device. <Back>: Return to previous menu without resetting the device.

Menu Item	Description
Manage Restore Point	Allows you to create, update or recall the Device Restore Point. A Device Restore Point is a saved copy of all device settings, allowing you to restore the device back to a known state or preferred configuration at any time. Note that there can only be one restore point on a device at a time. **Create**: Saves a new restore point if none already exists, copying all the device's current settings. **Update**: Overwrites the existing restore point with the device's current settings. **Recall**: Recalls the restore point and overwrites the current device settings with those saved in the restore point. <Back>: Return to previous menu.
Reset Security	Allows you to reset the device's security settings without affecting the rest of the device configuration. You will then be able to choose a new Security Mode for the device. After selecting this menu item you will be asked to **confirm** your decision, with a reminder that if DMX is currently active, it will be held at the current level until a new Security Mode is chosen.
Reboot	Will cause the device to soft reboot. After selecting this menu item you will be asked to **confirm** your decision.
<Back>	Return to previous menu.

PORT STATUS AND CONFIGURATION MENU

Port Status may be reviewed by turning the encoder knob to reach the desired port, from the main screen showing the device name and IP address. The LCD shows the following information.



The Port's soft label, configurable in Pathscape, is shown on the top line. By default, the label is the Port number.

Below that, the Port number and patch is shown.

If the Port is configured as an **Input**, it will show:

- **Port <x>: Universe #**: The Network DMX Universe the Port is set to transmit to

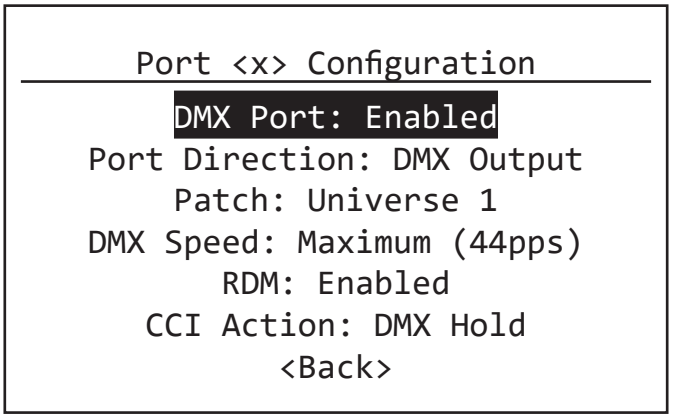
If the Port is configured as an **Output**, it will show:

- **Port <x>: Universe #**: The DMX512 Universe the Port is set to output to, if assigned a Standard Universe, or
- **Port <x>: Patch Name**: The name of the Custom Patch assigned to this Port, if applicable.

The bottom line shows the Port Status. It will show:

- **Status: Active Input/Output**: The Port is currently receiving DMX512 (if set to Input) or transmitting DMX512 (if set to Output).
- **Status: Inactive Input/Output**: The Port is not currently receiving DMX512 (if set to Input) or not currently transmitting DMX512 (if set to Output), however the Port is still enabled.
- **Status: Disabled Input/Output**: The Port is currently disabled.

From the Port Status screen of the desired Port, push the button. The Port Configuration menu will be shown.



Menu Item	Description
DMX Port	For debugging purposes or otherwise, you may want to disable a Port. All other properties will remain unchanged. Choose **Enabled** (default) or **Disabled.** If a Port is **Disabled**, its LED will shut off. <Back>: Return to previous menu.
Port Direction	Set the DMX direction for the selected Port. Choose **DMX Input** or **DMX Output** (default). <Back>: Return to previous menu.
Patch	Shows and allows selection of the patch for the selected Port. Scroll the list to choose from standard Universes, from 1 to 63999. You may also choose **Unpatched**. This is analogous to unplugging the DMX cable. The Port remains “On”, however no data is sent or received. For Output Ports: If you have previously set a **Custom Output Patch** using Pathscape, its name will be shown here. **NOTE** that you cannot select or create Custom Patches using the front panel. If you select a standard Universe, you will not be able to select the previously used Custom Patch again from the front panel, it will need to be set using Pathscape. <Back>: Return to previous menu.
DMX Speed:	Set the DMX Output speed. This has no effect on Input Ports. ANSI E1.11 compliant devices should be able to receive at Maximum speed (44 Hz), but some devices may require you to lower the number of DMX512 packets per second. The slowest rate is 30 Hz. Values are Maximum, Fast, Medium and Slow. **Slow**: 20 packets per second (pps) **Medium**: 37 pps **Fast**: 40 pps **Maximum**: 44 pps (Default) <Back>: Return to previous menu.

Menu Item	Description
RDM	Enable or Disable RDM functionality on the selected Port. **Enabled** (Default). When **disabled**, no Alternate Start Code packets will be sent on the DMX512 link. Non-RDM compliant devices may react badly to RDM packets <Back>: Return to previous menu.
CCI Action	Shows and allows selection of the Contact Closure Interface action. **None** (default): CCI does nothing. **DMX Hold**: CCI will force the DMX512 port to snapshot the current DMX levels and maintain them indefinitely, ignoring any further changes. Useful to lock out any unintended changes once levels are set as desired. **RDM Pause**: CCI will suspend all RDM discovery (quick or background), RDM GET and SET commands. Useful in a show-mode setting where RDM could negatively impact network performance <Back>: Return to previous menu.
<Back>	Return to previous menu.

APPENDIX 1: ELECTRICAL, COMPLIANCE & OTHER INFORMATION

ELECTRICAL INFORMATION

- Power input:
  - Power-over-Ethernet (PoE): Class 2 Device, 8W Maximum draw
  - Auxiliary DC input: 24-48VDC, 175 mA Maximum current draw
- DMX Ports:
  - 3000V isolation between DMX ports
  - 250V fault protection on DMX ports

COMPLIANCE

- ANSI E1.11 DMX512-A R2013
- ANSI E1.20 RDM - Remote Device Management
- ANSI E1.31 - streaming ACN, Art-Net, Strand ShowNet, Pathway ssACN
- ANSI E1.33 RDMnet - RDM over IP
- IEEE 802.3af Power-over-Ethernet
- California Title 1.81.26, Security of Connected Devices
- RoHS 2011/65/EU:2015/863
- CE

PHYSICAL

- Weight: 2.3 lbs (1kg) [base device, without attached rack mounting hardware]
- Dimensions: 8.6” W x 1.7” H x 7” D (218mm W x 43mm H x 178mm D) [base device, without attached rack mounting hardware]