



Pathport Hand Held DMX/RDM Ethernet Gateway



Model PWPP HH P1 XLR5F
Running Firmware version 6.2 or later

User Guide

October 2021



Copyright © Pathway Connectivity
A Division of Acuity Brands Lighting Canada (“Pathway”) and its licensors.
All rights reserved.

This software and, as applicable, associated media, printed materials and “on-line” or electronic documentation (the “Software Application”) constitutes an unpublished work and contains valuable trade secrets and proprietary information belonging to Pathway and its licensors.

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 HAND HELD - PWPP HH P1 XLR5F	1
PROTOCOLS SUPPORTED	1
DMX512.....	1
ETHERNET PROTOCOLS.....	1
REMOTE DEVICE MANAGEMENT (RDM).....	2
INSTALLATION INSTRUCTIONS.....	2
INSTALLATION ENVIRONMENT	3
POWER	3
REPLACING THE BATTERY	3
PANEL LAYOUTS	4
FRONT PANEL.....	4
LCD	4
BUTTON INTERFACE	4
RJ45 etherCON.....	5
DMX PORT	5
REAR PANEL	5
HANGING BRACKET	5
BATTERY COMPARTMENT	5
CONFIGURATION	6
SECURITY	7
BACKGROUND INFORMATION	7
WHAT THIS MEANS TO YOU	7
SECURITY DOMAINS	8
RED PADLOCK -  “Ready to Secure” device (previously “Unsecured”).....	8
AMBER PADLOCK -  “Other Domain” name showing device.....	8
AMBER PADLOCK -  “Read Only” (previously “Locally Secured”).....	8

GREEN PADLOCK -  “My Domain” shows devices in the current domain....	8
EMPTY SECURITY DOMAIN CELL – Firmware version prior to 5.0 - device shipped prior to January 1, 2020	8
CREATING A SECURITY DOMAIN	9
ADMINISTERING A DOMAIN	14
MANAGE SECURITY DOMAIN.....	14
MANAGE DEVICES.....	18
RECOVERING A DOMAIN	19
RETAINING DEVICE SETTINGS FROM UNKNOWN DOMAINS.....	21
USING OLDER VERSIONS OF PATHSCAPE WITH NEW DEVICES..	21
LOCAL CONFIGURATION ONLY - Using PWPP HH P1 without Pathscope.....	22
PATHWAY ssACN (Secure sACN)	24
DOMAIN AUTO ssACN PASSWORD.....	24
CUSTOM ssACN PASSWORD	24
CHOOSING PATHWAY ssACN AS NETWORK PROTOCOL.....	25
MANAGING PATHWAY ssACN PASSWORDS	26
SOFTWARE (PATHSCAPE) CONFIGURATION.....	29
NETWORK SETUP	29
DEVICE PROPERTIES.....	30
PATHWAY SECURITY DOMAIN.....	30
BASIC PROPERTIES	30
DEVICE INFO	31
NETWORK PROPERTIES	32
NETWORK PARTNER (LLDP).....	33
NETWORK DMX RECEIVE PROTOCOLS	33
NETWORK DMX TRANSMIT PROTOCOL	35
ADVANCED PROPERTIES.....	35
PATHPORT PORT PROPERTIES.....	36

OUTPUT PORT PROPERTIES	36
BASIC PROPERTIES	36
DEVICE INFO	37
STATUS	37
DMX512 PORT PROPERTIES	37
PORT PATCH	38
NETWORK DMX PROPERTIES	39
SIGNAL LOSS	39
RDM PROPERTIES	40
INPUT PORT PROPERTIES	41
BASIC PROPERTIES	41
STATUS	41
DMX512 PORT PROPERTIES	42
PORT PATCH	42
NETWORK DMX PROPERTIES	42
SIGNAL LOSS	43
RDM PROPERTIES	43
PATCHING PORTS	43
UPDATING DEVICE FIRMWARE	44
FACTORY DEFAULT	45
FRONT PANEL UI AND MENU	46
BEFORE YOU START	46
FRONT PANEL UI	46
SETTING SECURITY MODE	47
MAIN DISPLAY MESSAGES	47
USING THE FRONT PANEL UI	48
MENUS	48
GATEWAY CONFIG	48
PORT CONFIG	50
NETWORK CONFIG	51

DMX PORT MONITOR.....	51
RDM TOOLS	52
TEST DMX OUTPUT	53

APPENDIX 1: ELECTRICAL, COMPLIANCE & OTHER INFORMATION
.....55

ELECTRICAL INFORMATION.....	55
COMPLIANCE	55
PHYSICAL.....	55

ABOUT PATHPORT HAND HELD - PWPP HH P1 XLR5F

Pathway Connectivity's **PWPP HH P1 XLR5F** is a single-port DMX-over-Ethernet gateway intended for use primarily in entertainment lighting systems. The PWPP HH P1 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 HH P1 may be used alone, networked with other Pathport gateways, as well as with a number of other Ethernet-aware lighting control products, such as consoles and controllers.

The PWPP HH P1, 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 HH P1 is easily configured and upgraded using the freely available software tool, **Pathscape**. It is also configurable using the Front Panel, which consists of the LCD and a 3-button interface. **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 HH P1 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 it 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 HH P1 is fully compliant with Net3, and will seamlessly receive either Final Draft 20, or the ANSI approved versions of sACN.

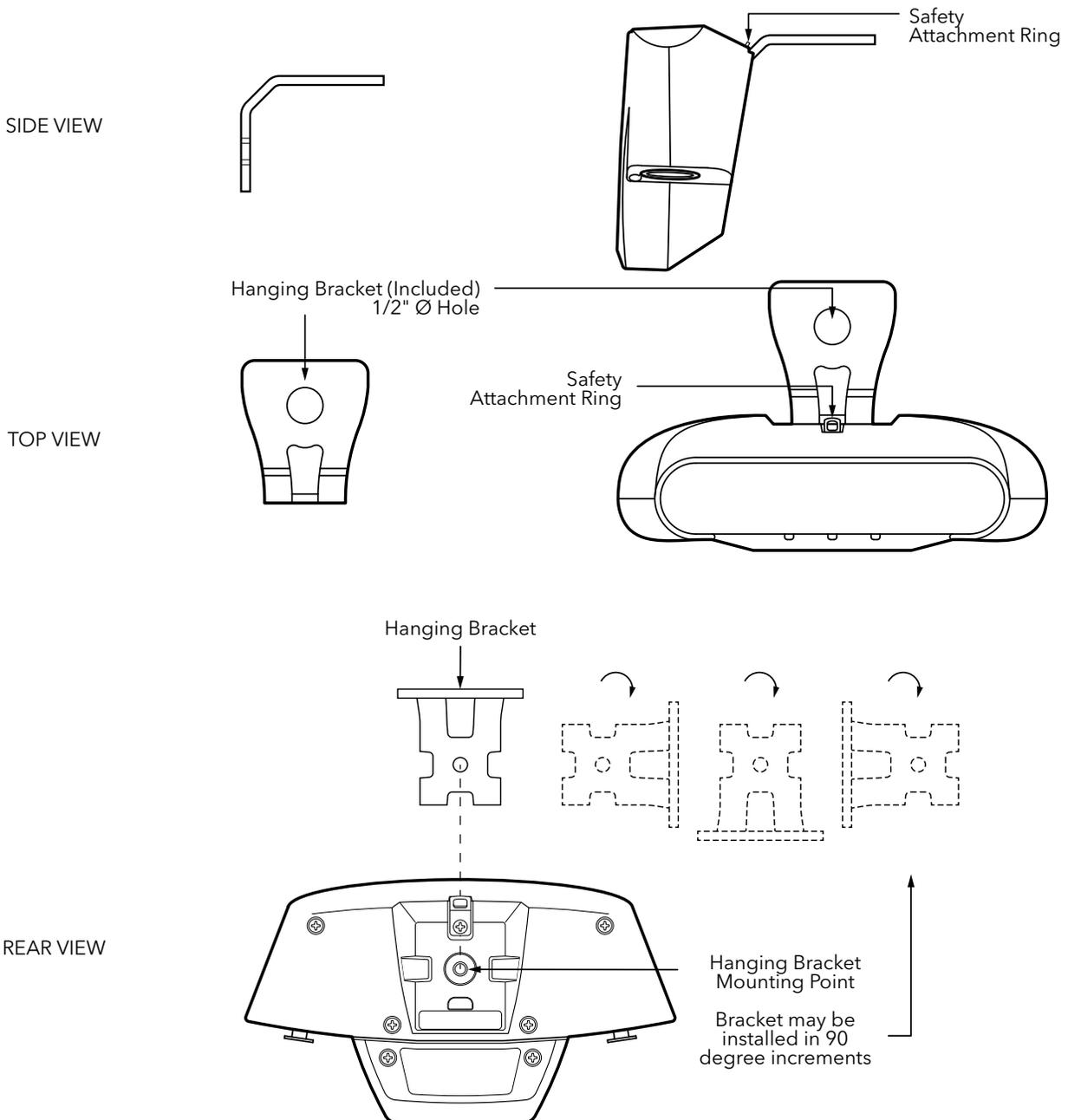
Pathway ssACN (Secure sACN): A new protocol developed by Pathway Connectivity that incorporates many features of ANSI E1.31 sACN, but adds a layer of secure authentication. See later in the manual for details on Pathway ssACN.

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 HH P1 will route. The free downloadable Pathscape software is required to use the PWPP HH P1 as an RDM gateway to configure DMX-based equipment.

INSTALLATION INSTRUCTIONS

The PWPP HH P1 is intended for hand held use during configuration of a system, or can be mounted using the included hanging bracket.



The rear-mounted hanging bracket accepts a 1/2" (12.5mm) bolt, and is intended to be suspended using a standard C-clamp or similar pipe hanger. A separate anchor point is provided for a secondary safety. The bracket may be installed in 90 degree increments as needed.

The PWPP HH P1 has an IP54 enclosure rating **when mounted so the cable connections point directly downward.**

INSTALLATION ENVIRONMENT

The PWPP HH P1 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: All ports on the PWPP HH P1 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.

POWER

The PWPP HH P1 will operate on IEEE 802.3af Power-over-Ethernet (PoE) as a class 1 device, drawing less than 5 Watts. It will also operate on a standard 9V battery (included, already installed in device).

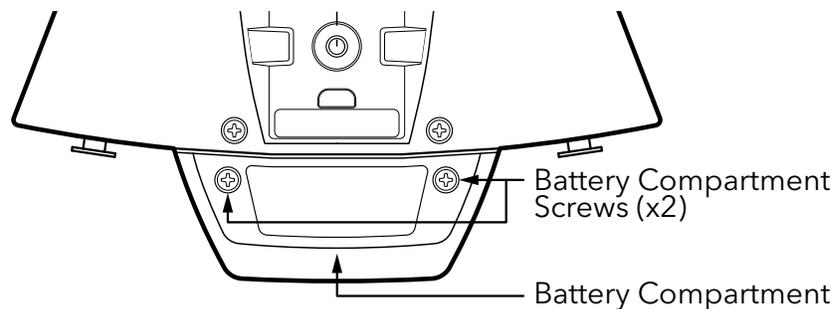
The gateway will automatically sense the presence of PoE and will use it rather than the battery. However, the device will not automatically switch to battery power if PoE is subsequently lost or disabled.

When operating on battery power, the PWPP HH P1 will shut down after 30 seconds without a button push, to conserve the battery. One 9V battery will provide at least 30 minutes of configuration operations. The PWPP HH P1 is not intended to be used extensively or permanently on solely battery power. For normal show operation, the device is intended to run on PoE.

REPLACING THE BATTERY

Disconnect any PoE source before replacing the battery.

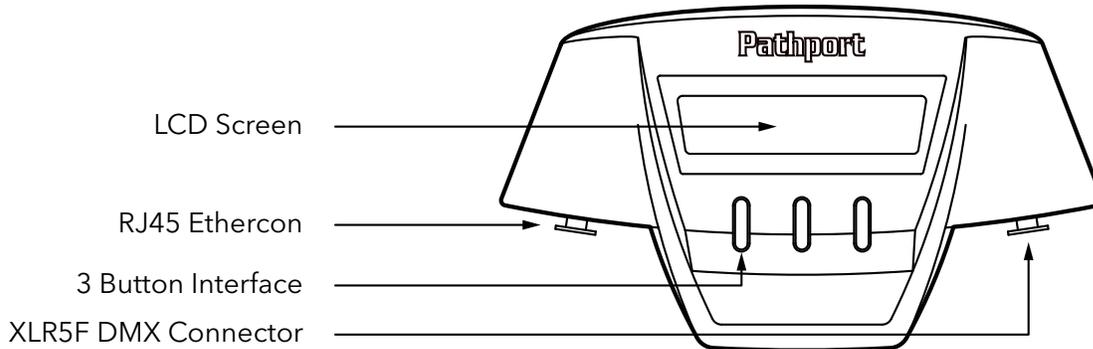
To replace the internal battery, remove the two battery compartment screws on the bottom rear of the gateway.



Disconnect the battery from the connector, and replace with a fresh 9V battery, observing the polarity of the contacts. Replace the cover and re-tighten the battery compartment screws.

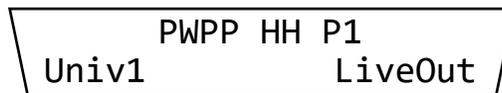
PANEL LAYOUTS

FRONT PANEL



LCD

The Pathport Hand Held has a 2-line, 16-character backlit LCD.



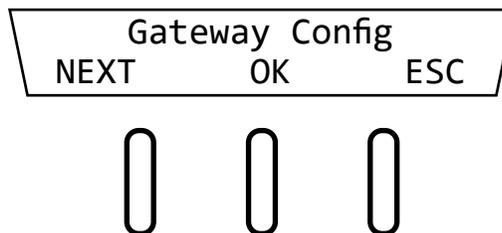
The upper line of the display will show the gateway's name (if set in Pathscape), or the device's IP address. The lower line will show the Universe number or patch name and the DMX status.

By default, the backlight is off, except when pressing any of the 3 buttons. Pressing any button again will enter the menu system.

If desired, the backlight can be set to be always on, by setting a property in Pathscape. See **Software Configuration** below for more information.

BUTTON INTERFACE

The three buttons below the LCD provide menu navigation.



Typically, the leftmost button is "NEXT" and will cycle through menu items. The middle button is "OK" and will accept the currently selection option or enter the next menu level. The rightmost button is "ESC" and will exit out of the current menu item, or return to the previous menu level, without making changes.

Configuration changes must be saved by pressing the "SAVE" button to take effect. Pressing the ESC button or allowing battery timeout will cause changes to be lost.

See further sections for information on battery timeout and menu navigation.

RJ45 etherCON

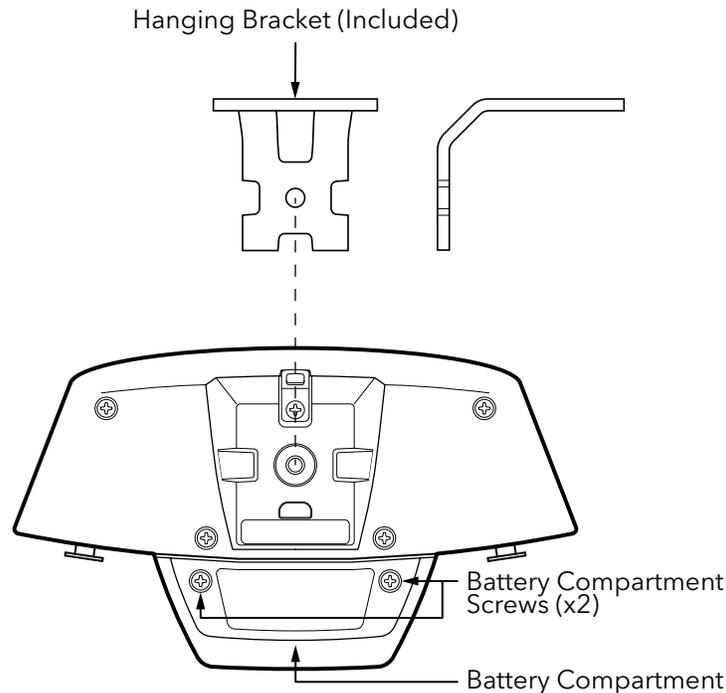
On the left side of the device is the RJ45 etherCON port, which will accept a standard male RJ45 or Neutrik etherCON connector for connecting to the lighting network. The PWPP HH P1 can be powered via PoE.

The amber LED next to the RJ45 port will glow with link activity.

DMX PORT

On the right side of the device is the DMX port, a 5-pin female locking XLR connector. The female XLR indicates the gateway is natively a DMX output device, but the port direction can be changed to an Input as well. The green LED next to the DMX port indicates active DMX input or output, depending on the DMX port direction.

REAR PANEL



HANGING BRACKET

As shown above, the rear of the PWPP HH P1 has a mounting location for the hanging bracket. The bracket itself can be rotated in 90 degree increments to accommodate different device orientations, as needed.

BATTERY COMPARTMENT

The battery compartment is located below the mounting bracket. As shown above, to access the battery for replacement, remove the two screws and remove the compartment cover. Disconnect the battery from the connector and replace with a fresh battery, observing the correct polarity.

CONFIGURATION

The PWPP HH P1 may be configured from the front panel using the LCD and three-button interface. However, we recommend using our free software tool, Pathscape, when possible. 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 buttons 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. This is not applicable to the PWPP HH P1.

SECURITY DOMAINS

To simplify the process of managing security on your network, Pathscope 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 Pathscope there is a column that shows you the name of the devices’ domain and a **padlock icon** showing their current state.

Select View: * DEFAULT Filter: Search:

Status	Security Domain	Name	Type	IP Addr
Online	Studio	Rack PWPP RM P4	Pathport 4-port Rack-mount	10.1.139.227
Online	Studio	Rack PWPP RM P8	Pathport 8-port Rack-mount	10.6.27.72
Online	Ready to Secure	Rack PWPP DIN P2	Pathport 2-port DIN-mount	10.0.79.235
Online	pathway	[blank](10.0.84.106)	Pathport 2-port DIN-mount	10.0.84.106
Online	pathway	[blank](10.30.132.120)	VIA 16-port PoE Ethernet Switch	10.30.132.120

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

Status	Security Domain
Online	Stage
Online	Ready to Secure
Online	Ready to Secure
Online	Ready to Secure
Online	Read Only
Online	Disabled by User
Online	24WML

RED PADLOCK - “Ready to Secure” device (previously “Unsecured”)

Prior to Pathscope 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 Pathscope 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 Pathscope, you **must Reset Security** settings from the front panel and then add it to the Security Domain using Pathscope.

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

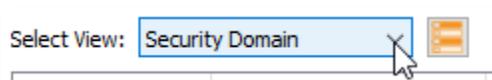
Once you have logged into a Security Domain with a password, any device in your domain will appear with a green padlock and all their properties will be Read/Writable.

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. Pathscope 4 will be able to read and write properties exactly like earlier versions of Pathscope. 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

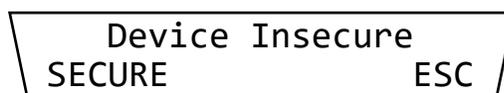
- After starting Pathscape, the online devices will populate the Device View.
- Choose the **Security Domain** view from the **Select View** dropdown



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

Status	Security Domain	Name	Type
> Online	Ready to Secure	Rack PWPP RM P8	Pathport 8-port Rack-mount
> Online	Ready to Secure	Rack PWPP DIN P2	Pathport 2-port DIN-mount
> Online	Ready to Secure	Rack PWPP RM P4	Pathport 4-port Rack-mount

- **NOTE:** PWPP HH P1 units running **V6.1 firmware or later** will show a **Device Insecure** screen on the front panel LCD, if attempting to enter the main menu (pressing any button twice).

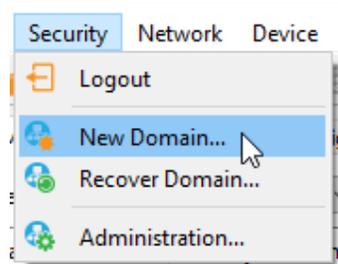


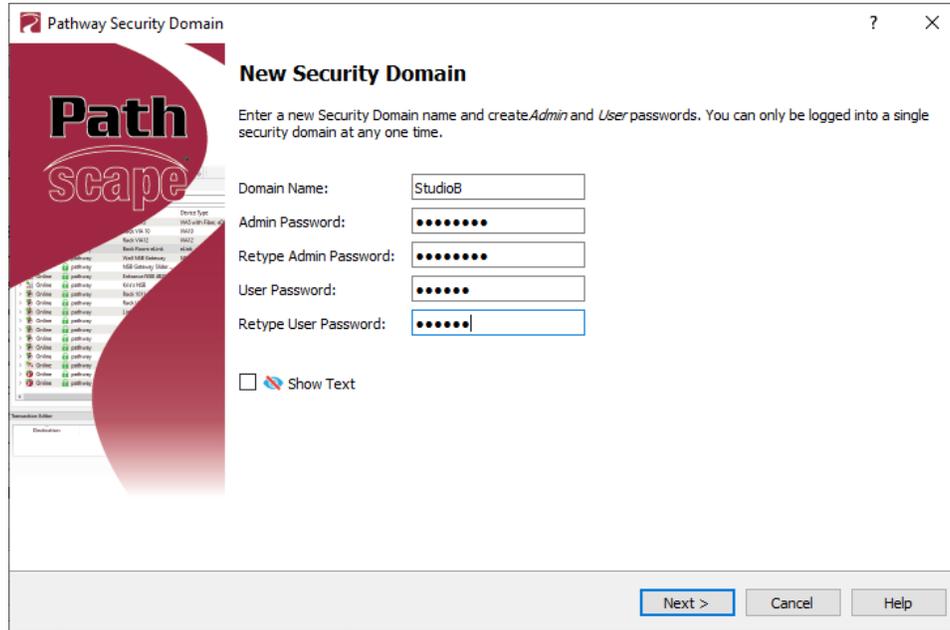
- **No action is required** here to add the device to Pathscape.
- If you wish to configure the device only via the front panel, clicking the left button to select **SECURE** will put the unit into **Local Configuration Only** mode. In this mode, the device cannot be added to a Pathscape Security Domain, but will be secure from attempts to change configuration settings from the network.

More information on Local Configuration Only mode later in this manual.

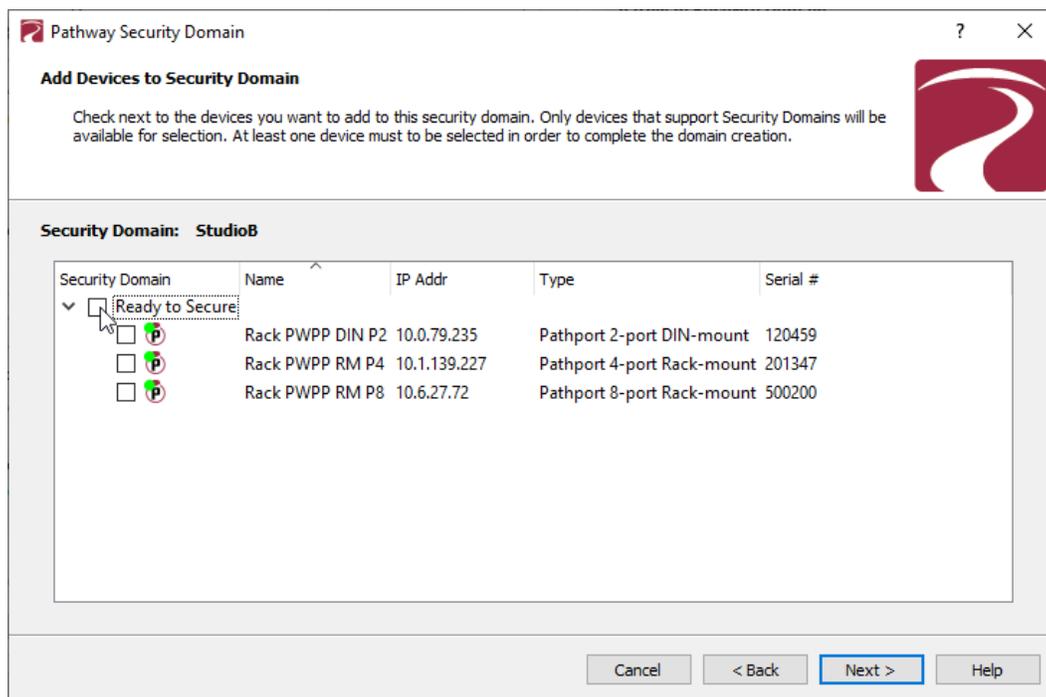
- If your devices have old firmware, you may update them to current firmware by going to the **Tools** menu in Pathscape and selecting **Firmware Updater**. Select the devices to upgrade, and choose **Select Latest**, then **Send Firmware**. (See the **Upgrading Device Firmware** section for more detail). 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**.

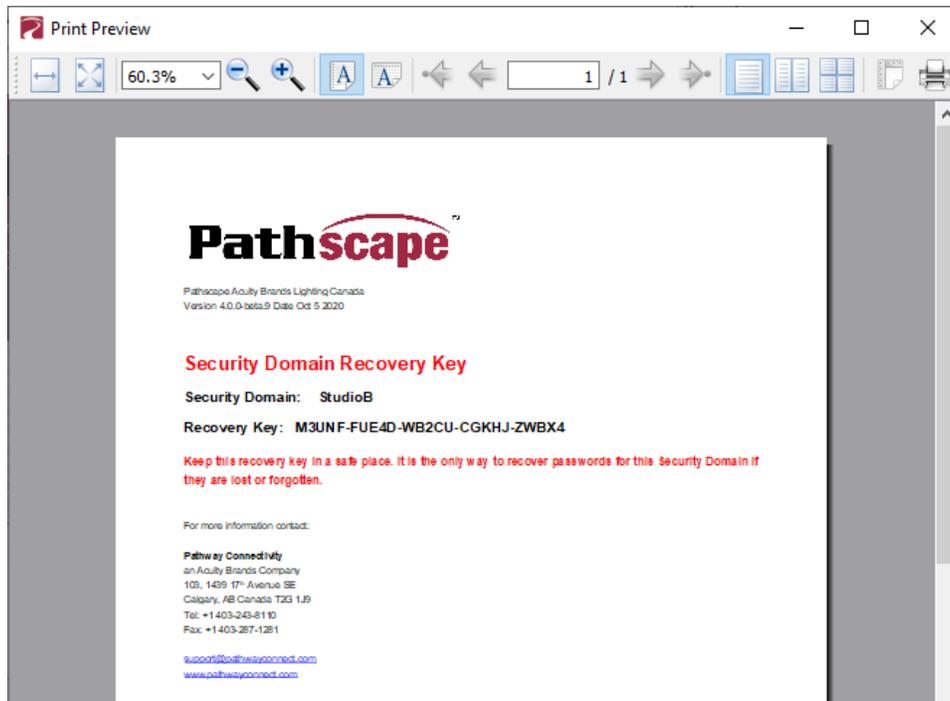


- The next window will show the **Recovery Key**. This key will allow you to recover Security Domain access should the passwords be lost or forgotten.

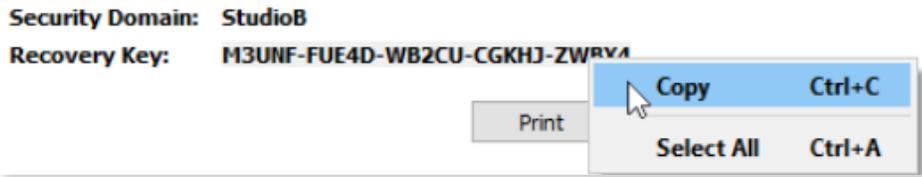
It is extremely important to keep a record of this Recovery Key, as this is the only time it will be shown to you. Print the Recovery Key.



- 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.

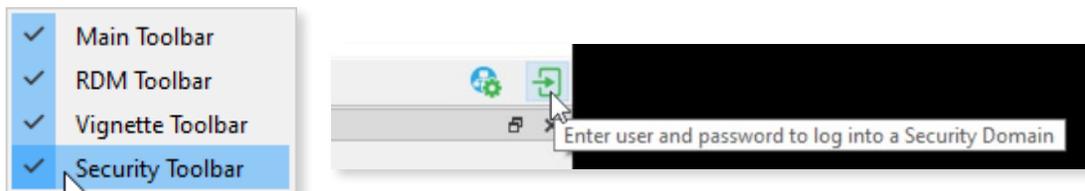
Managers of the facility should store this key in a safe place, keeping in mind that anybody with this key can change both the Administrator and User passwords at any time.



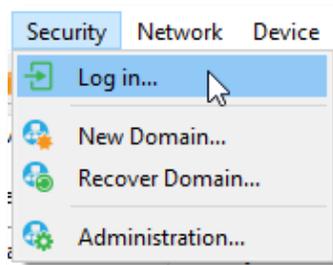
- Click **Finish** and the window will close, and the devices will be added to the domain. The devices will have an **amber padlock** and their properties will be read-only.

Status	Security Domain	Name	Type
> Online	StudioB	Rack PWPP RM P4	Pathport 4-port Rack-mount
> Online	StudioB	Rack PWPP RM P8	Pathport 8-port Rack-mount
> Online	StudioB	Rack PWPP DIN P2	Pathport 2-port DIN-mount

- 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.

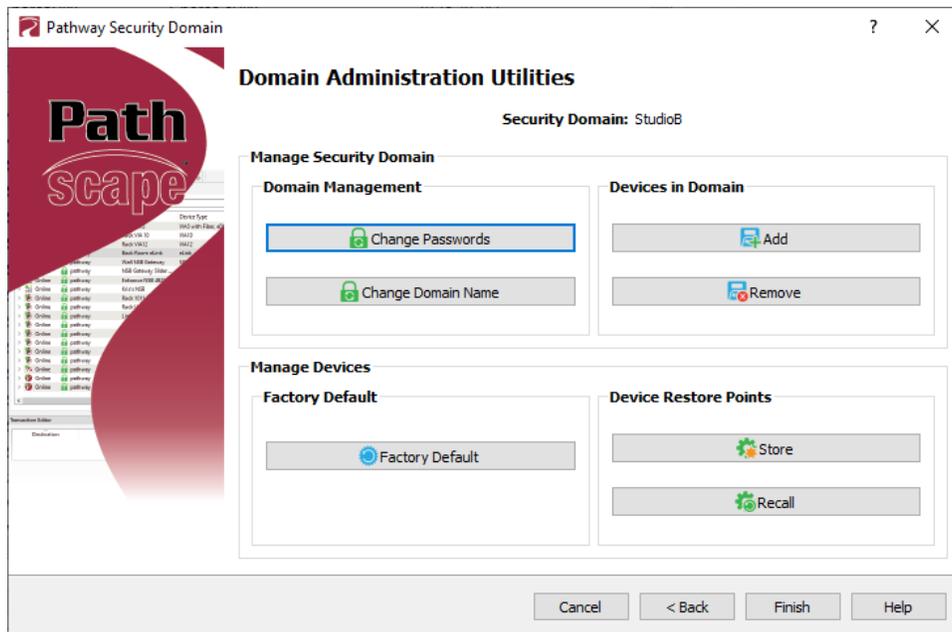


ADMINISTERING A DOMAIN

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



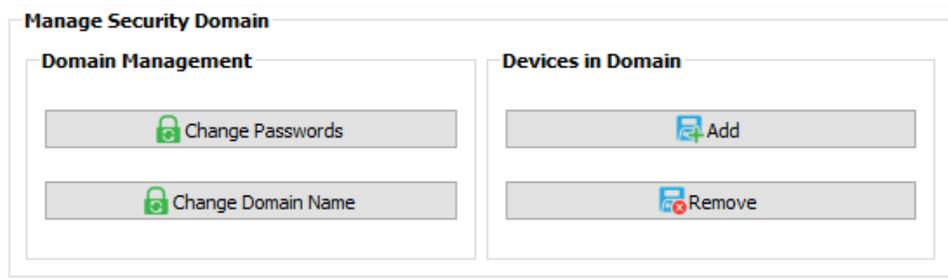
Enter the **Admin** password for the Security Domain, and the **Domain Administrator Utilities** window will appear.



The Domain Admin Utilities window is broken down into two 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

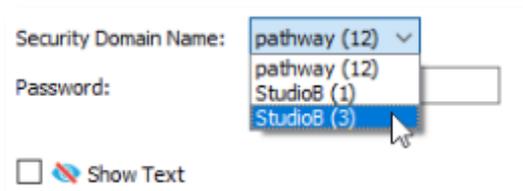
If your staffing changes, it is a good idea to change the passwords on the domain. Click this button to change the current Security Domain Admin and User passwords. **All devices should be online when you change the password.**



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 coincidentally 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**.

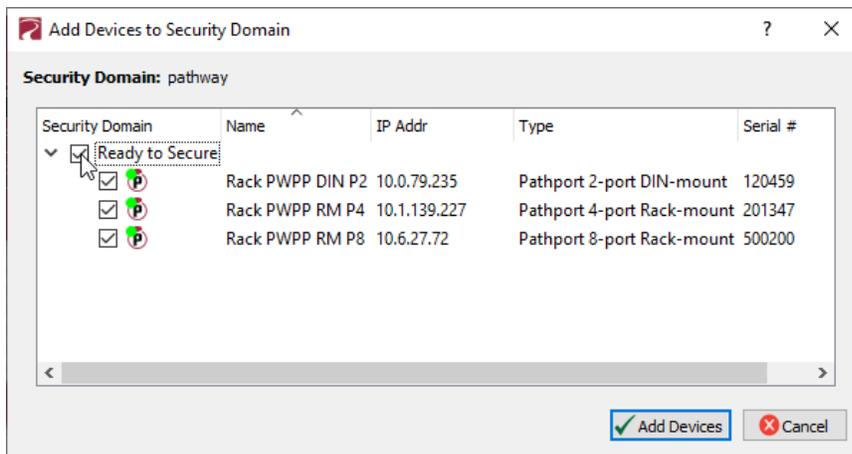
The window will close, and you will be logged out of the current domain, and the Domain Name will be changed to the new value. **You will have to log into the Domain again** to make any further changes.

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

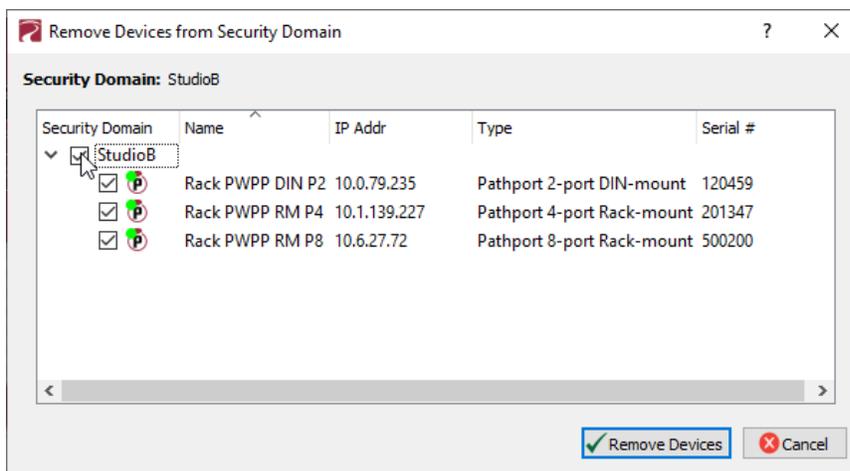
Clicking on this button will bring up the **Add Devices** window, where Ready to Secure devices can be added to the current Security Domain.



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

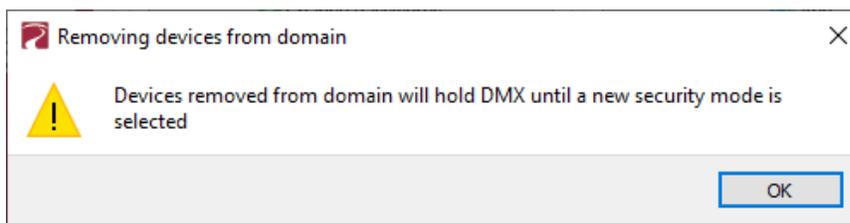
Click this button to remove devices from the current Security Domain.



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.

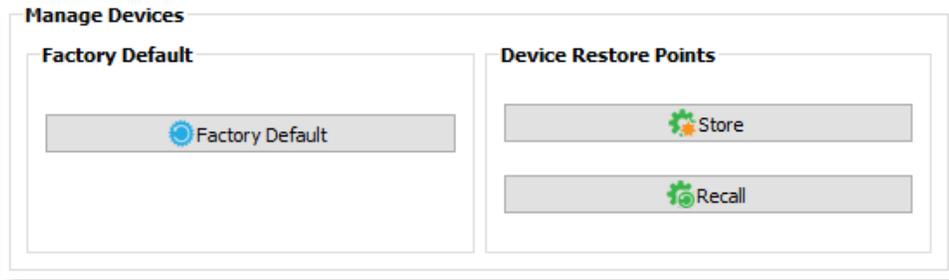
Note: When a device is removed from a domain, a window will appear reminding you that any active Network DMX levels will be held by that device until a new security mode is selected.



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**.



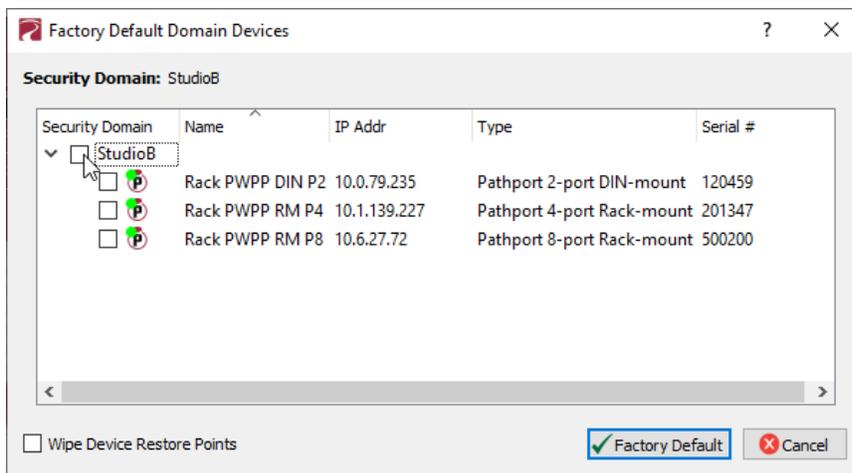
FACTORY DEFAULT

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.

Search the Pathway website for **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.

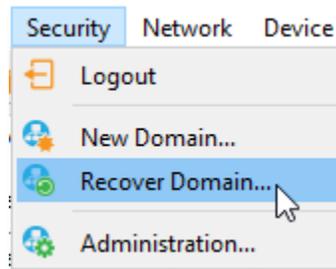
DEVICE RESTORE POINTS

Not applicable to PWPP HH P1.

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

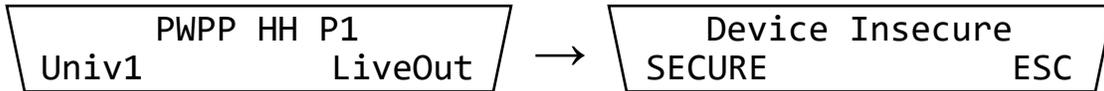
If you use Pathscape 1 or Pathscape 2 with devices shipped after **January 1, 2020 (Version 5 firmware or later)**, you will not be able to configure them. **You must use Pathscape 4 or later**. As a reminder, the device label will appear in the earlier versions of Pathscape as **"Use latest Pathscape 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 HH P1 without Pathscope

The PWPP HH P1 has features that use unsecured protocols. You may not intend to use Pathscope, 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 HH P1, but are not using Pathscope to add your devices to a **Security Domain**.

Enter **Local Configuration** mode by selecting **SECURE** from the main menu.

This menu is shown upon pressing any button twice, 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.



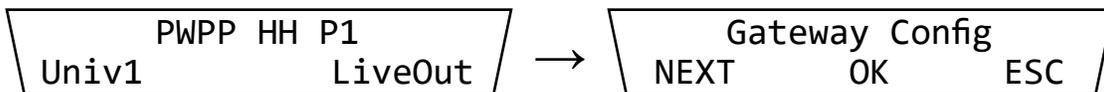
Main menu. Press any button twice to enter menu structure and see the Device Insecure screen.

- From the **Device Insecure** menu shown on the LCD, press the left button to select **SECURE**. You will then have full access to the menus.
- In Local Configuration / Read Only mode, **Pathway ssACN** (Secure sACN) will not function.

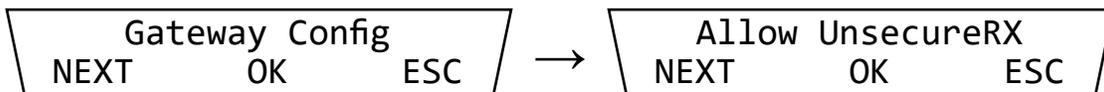
Pathway ssACN uses the **ssACN Password** to communicate with other devices on the same Domain. In Local Configuration Only mode, the device generates a random secret password that is never accessible by the user for its own “Local Domain”.

The menu item for Pathway ssACN may still be displayed in this mode, and you may be able to set this item to “Enabled”, but note that **Pathway ssACN will not function in Local Configuration / Read Only mode**.

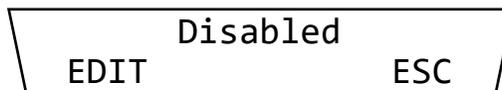
- To use other standard (unsecured) protocols, you **must manually enable them**.
 - Press any button twice to enter the main menu.



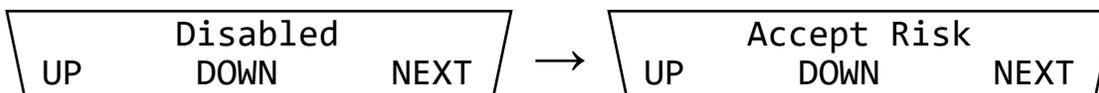
- The first menu item will be **Gateway Config**. Press the **OK** (middle) button.
- The first item shown in this menu will be Factory Default. Press the **NEXT** (left) button to go to the next menu item, **Allow UnsecureRX**, and press the **OK** button.



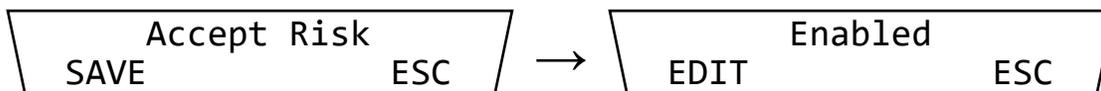
- The next screen will show the current status of the Allow UnsecureRX property. By default, this is **Disabled**.



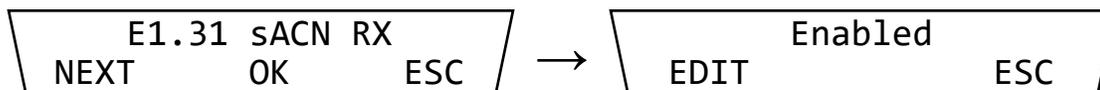
- Press the **EDIT** (left) button. The current value will begin flashing, and the bottom row of the LCD will show the options **UP**, **DOWN** and **NEXT**. Press either the UP or DOWN buttons to change the current value to Accept Risk, then press the **NEXT** button.



- The next screen will allow you to **SAVE** the new value for this property, or **ESC** or cancel and return to the previous level.



- Once saved, return to the **Gateway Config** menu and cycle through menu items to find the Receive Protocols you wish to enable: **Pathport RX**, **ShowNet RX**, **ETC Net2 RX**, **Art-Net RX**, and **E1.31 sACN RX**.



- Configure the **Port Direction** to Input or Output and patch a standard universe (i.e., UNIV 1). See the **Front Panel UI and Menu** section for details on how to use the other menu functions.

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 **Factory Default** settings, then use Pathscape to add it to a Security Domain.

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**.

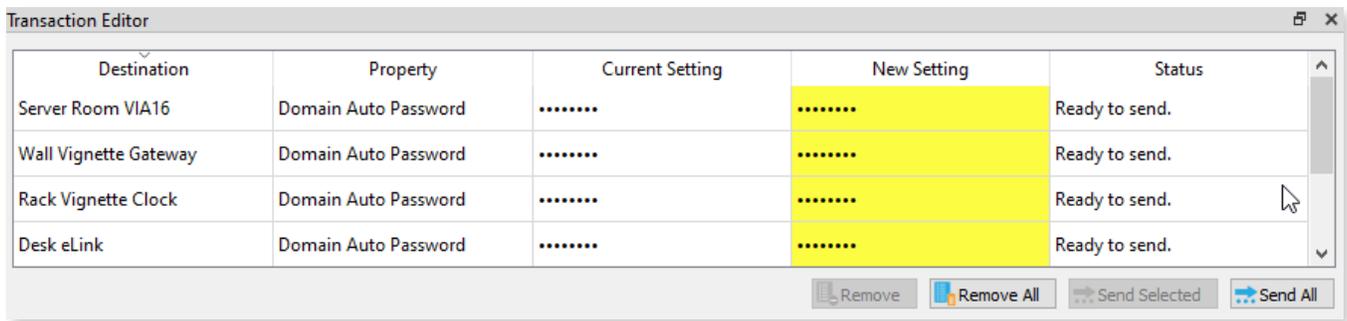
Receiving devices, like Pathport DMX/RDM gateways, share a **secret password** with known controllers in the venue, to verify the data source before driving the lighting rig. A cryptographic hash message is added to each E1.31 packet, verifying the authenticity of the source and the sequence of the data. 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.



Destination	Property	Current Setting	New Setting	Status
Server Room VIA16	Domain Auto Password	Ready to send.
Wall Vignette Gateway	Domain Auto Password	Ready to send.
Rack Vignette Clock	Domain Auto Password	Ready to send.
Desk eLink	Domain Auto Password	Ready to send.

Buttons: Remove, Remove All, Send Selected, Send All

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.

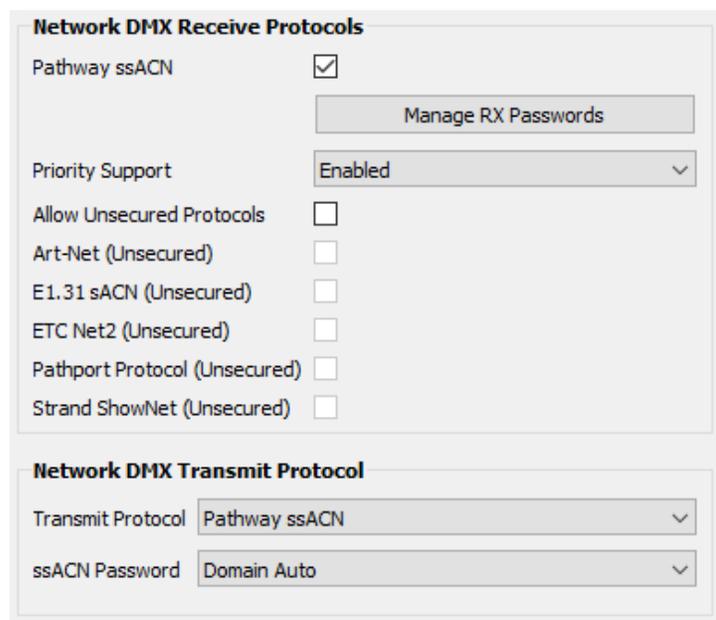
There may be other situations where a custom ssACN password is useful, but we recommend using the Domain Auto password for most systems unless you have unique requirements like the above.

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.

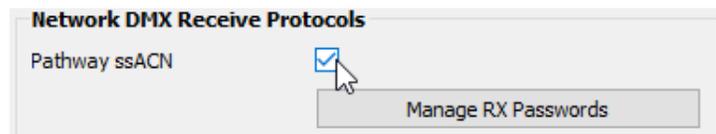
In the relevant devices' **base device** properties, there are two sections called **Network DMX Receive Protocols** and **Network DMX Transmit Protocol**.



The image shows two configuration panels. The top panel, titled "Network DMX Receive Protocols", contains the following settings: "Pathway ssACN" is checked; "Priority Support" is set to "Enabled"; "Allow Unsecured Protocols" is unchecked; "Art-Net (Unsecured)", "E1.31 sACN (Unsecured)", "ETC Net2 (Unsecured)", "Pathport Protocol (Unsecured)", and "Strand ShowNet (Unsecured)" are all unchecked. A "Manage RX Passwords" button is located below the "Pathway ssACN" checkbox. The bottom panel, titled "Network DMX Transmit Protocol", contains: "Transmit Protocol" set to "Pathway ssACN" and "ssACN Password" set to "Domain Auto".

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.

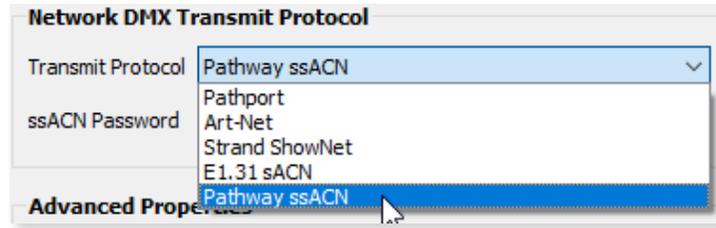
In the **Network DMX Receive Protocol** section, simply check the Pathway ssACN checkbox. We recommend unchecking the Allow Unsecured Protocols checkbox, if previously checked, since end devices can receive **both** ssACN and unsecured protocols if left checked.



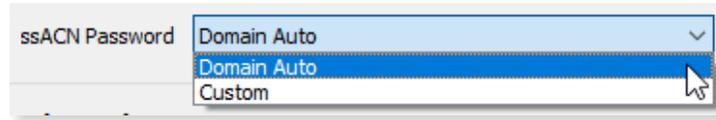
This is a close-up of the "Pathway ssACN" checkbox in the "Network DMX Receive Protocols" section. The checkbox is checked, and a mouse cursor is pointing at it. The "Manage RX Passwords" button is visible below it.

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.

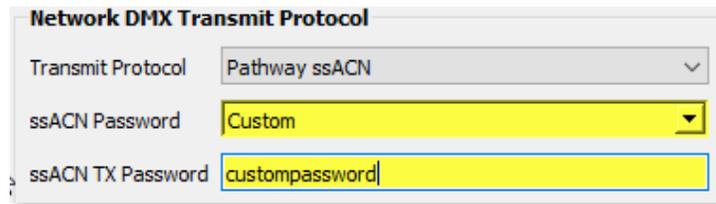


Once you select **Pathway ssACN**, the **ssACN Password** drop-down menu will appear.



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.

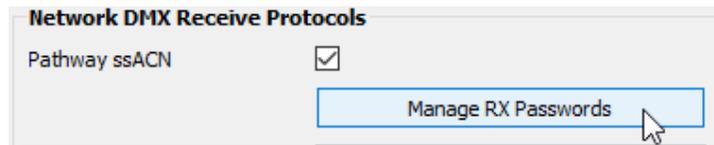
MANAGING PATHWAY ssACN PASSWORDS

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.

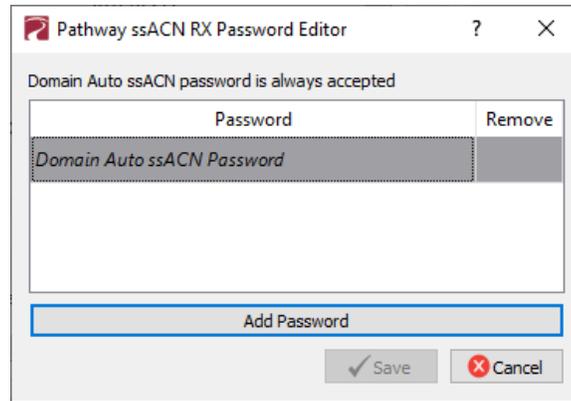
If you are using custom Pathway ssACN passwords, you will need to tell those devices transmitting Pathway ssACN what password to use, as well the devices that are receiving it what passwords to accept.

RX (RECEIVE) PASSWORDS

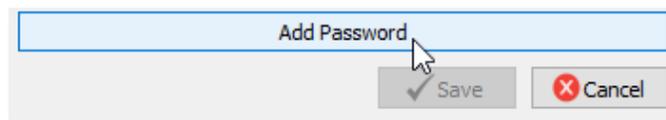
Under the checkbox for **Pathway ssACN**, there is the **Manage RX Passwords** button.



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.



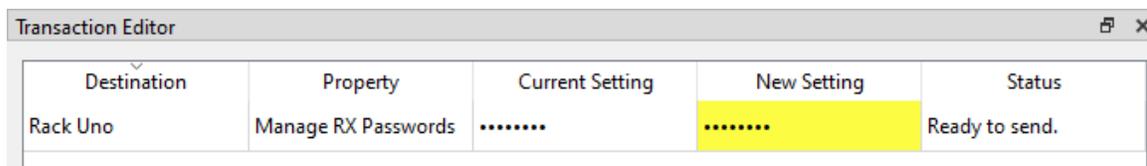
A blank entry will be added to the window.



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  button. A transaction will be queued in the Transaction Editor, which must be sent to save changes.

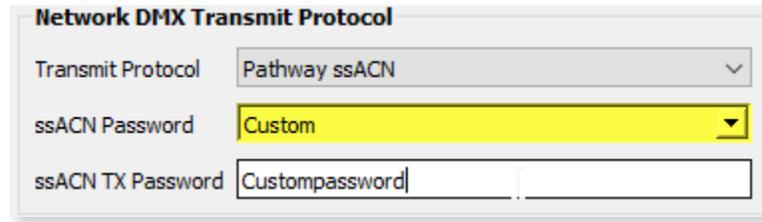


Click the  button to close the window without saving any changes or edits made.

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.



Network DMX Transmit Protocol

Transmit Protocol	Pathway ssACN
ssACN Password	Custom
ssACN TX Password	Custompassword

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 Pathscope to configure your PWPP HH P1. For in-depth information on using Pathscope, see the Pathscope manual. Pathscope is available for macOS and Windows from the Pathway website.

If using a PC with Pathscope 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 HH P1 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 HH P1'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 HH P1's default name in the device list will be shown as its IP address. Give it a useful name before continuing.

Status	Security Domain	Name	Type	IP Addr
>  Online	 pathway	PWPP HH Office	Pathport 1-port Hand Held	192.168.1.35

Basic Properties

Identify Device

Name

Notes

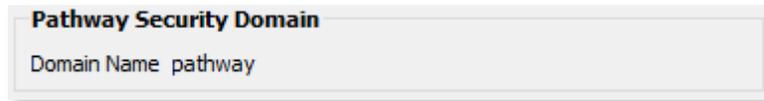
LCD Backlight

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

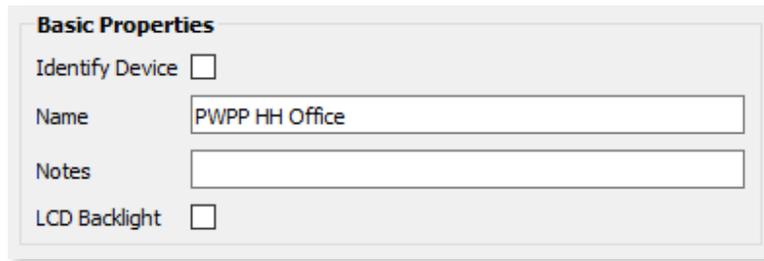


Pathway Security Domain
Domain Name pathway

DOMAIN NAME

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

BASIC PROPERTIES



Basic Properties

Identify Device

Name PWPP HH Office

Notes

LCD Backlight

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.

LCD BACKLIGHT

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

DEVICE INFO

Device Info	
Device Type	Pathport 1-port Hand Held
Network Interface	Ethernet
Firmware Version	6.2.0-rc.9
Serial Number	PP419267
MAC Address	00:04:a1:04:df:23

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.

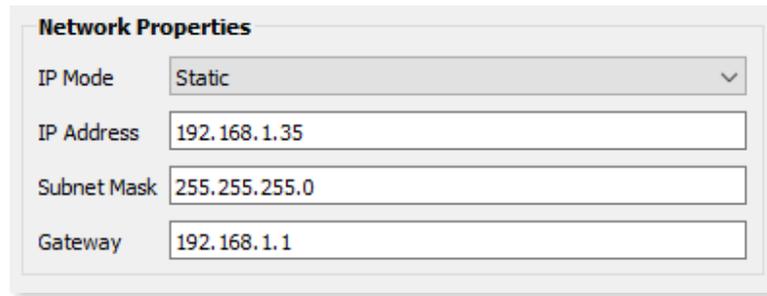
SERIAL NUMBER

Factory-set unique identifier. Read-only.

MAC ADDRESS

Factory-set hardware address. Read-only.

NETWORK PROPERTIES



The screenshot shows a 'Network Properties' dialog box with the following fields:

Network Properties	
IP Mode	Static
IP Address	192.168.1.35
Subnet Mask	255.255.255.0
Gateway	192.168.1.1

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 necessary.

NETWORK PARTNER (LLDP)

Network Partner (LLDP)

Partner Name VIA 12-Port Touring

Partner Port 3

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

Network DMX Receive Protocols

Pathway ssACN

Manage RX Passwords

Priority Support Enabled ▾

Allow Unsecured RX

Art-Net (Unsecured)

E1.31 sACN (Unsecured)

ETC Net2 (Unsecured)

Pathport (Unsecured)

ShowNet (Unsecured)

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 HH P1 respects the sACN priority (1-200) in the Universe header. Options are **Enabled** (default) or **Disabled**. Applicable to sACN or ssACN only.

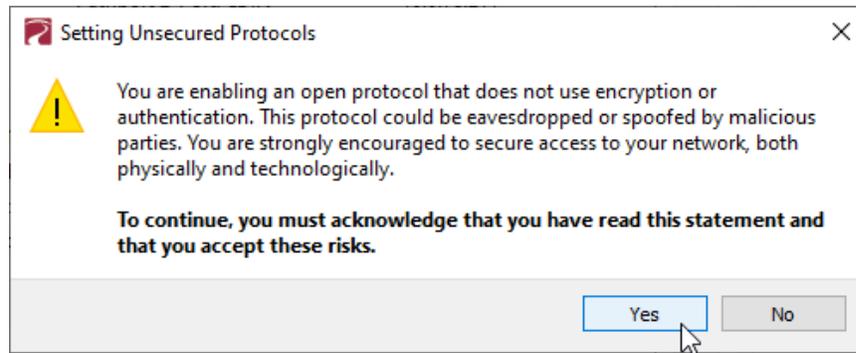
ALLOW UNSECURED PROTOCOLS

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 HH P1 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.

ETC Net2 (UNSECURED)

Check this box to enable the receiving of ETC Net2. You must check both the **Allow Unsecured Protocols** checkbox and this checkbox to use ETC Net2.

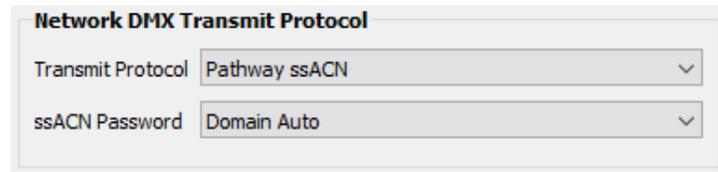
PATHPORT PROTOCOL (UNSECURED)

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



The screenshot shows a control panel titled "Network DMX Transmit Protocol". It contains two dropdown menus. The first is labeled "Transmit Protocol" and is set to "Pathway ssACN". The second is labeled "ssACN Password" and is set to "Domain Auto".

TRANSMIT PROTOCOL

Use the drop-down menu to select the network protocol the PWPP HH P1 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.

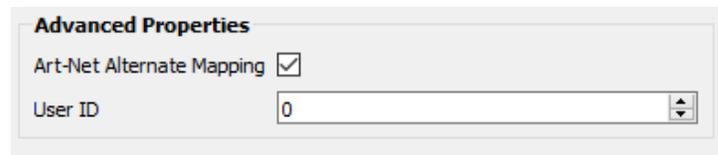
Pathway ssACN will use Pathway's secured sACN for transmitting to the network.

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.

ADVANCED PROPERTIES



The screenshot shows a control panel titled "Advanced Properties". It contains a checkbox labeled "Art-Net Alternate Mapping" which is checked. Below it is a text input field labeled "User ID" with the value "0".

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.

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.

Status	Security Domain	Name	Subdev #	Type
Online	pathway	PWPP HH Office		Pathport 1-port Hand Held
		Port A	A	DMX Port

OUTPUT PORT PROPERTIES

Basic Properties

Name: Port A

Notes: Out to Rig

Device Info

Device Type: DMX Port

Status

Network DMX: Inactive

DMX512: Inactive

DMX512 Port Properties

DMX512 Enable: Enabled

Port Direction: Output

DMX512 Output Speed: Maximum

Crossfade Enable:

Port Patch

Output Patch: Univ 1

 Custom Universe

Network DMX Properties

sACN Per-Channel Priority:

Signal Loss

Hold Forever:

Hold Time (s): 5.000

Fade to Black:

Fade Time (s): 5.000

Port Shutdown:

RDM Properties

E1.20 RDM Enable:

E1.20 RDM Background Discovery:

RDM Device Count: 0

RDM Pause:

Time Since Last Discovery: Discovery never run

BASIC PROPERTIES

Basic Properties

Name: Port A

Notes: Out to Rig

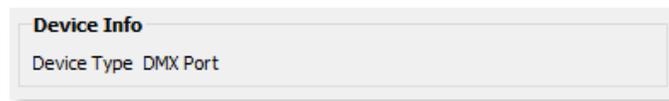
SUBDEVICE NAME

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 (if the Notes column is displayed).

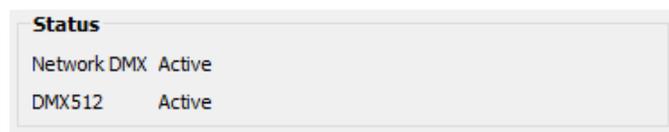
DEVICE INFO



DEVICE TYPE

Shows the Device Type for the currently selected device/subdevice. In this case, the subdevice is a DMX Port. Read-only.

STATUS



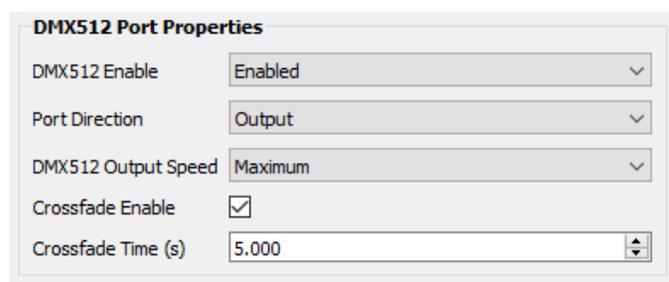
NETWORK DMX

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**.

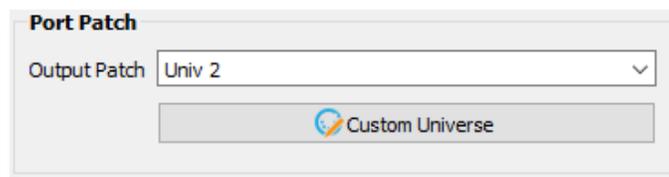
CROSSFADE ENABLE

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**.

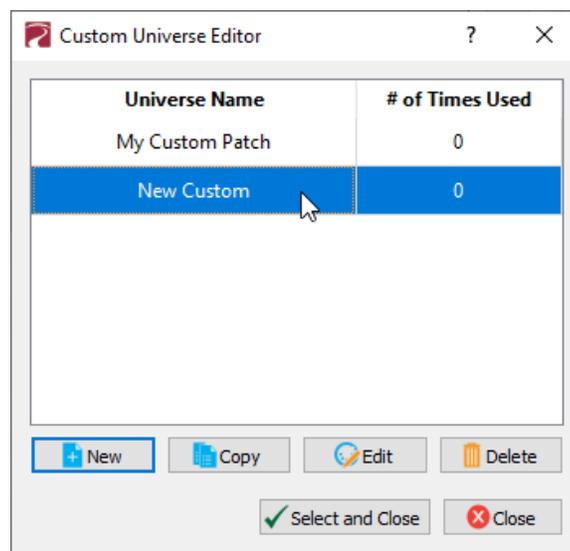
PORT PATCH



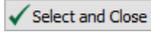
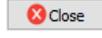
OUTPUT PATCH

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.

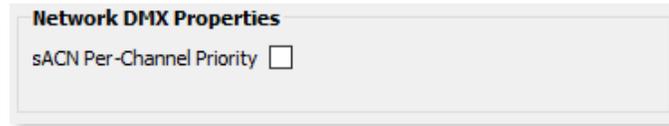
Click the  **Custom Universe** button to open the Custom Universe Editor.



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  to set the port to that patch. Click the  button to discard changes.

NETWORK DMX PROPERTIES

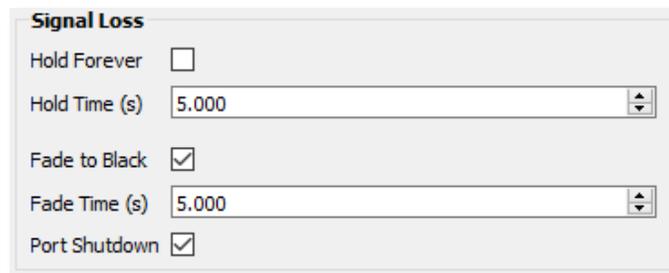


sACN PER-CHANNEL PRIORITY

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

RDM Properties	
E1.20 RDM Enable	<input checked="" type="checkbox"/>
E1.20 RDM Background Discovery	<input type="checkbox"/>
RDM Device Count	2
RDM Pause	<input type="checkbox"/>
Time Since Last Discovery	25 seconds

Pathscope 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.

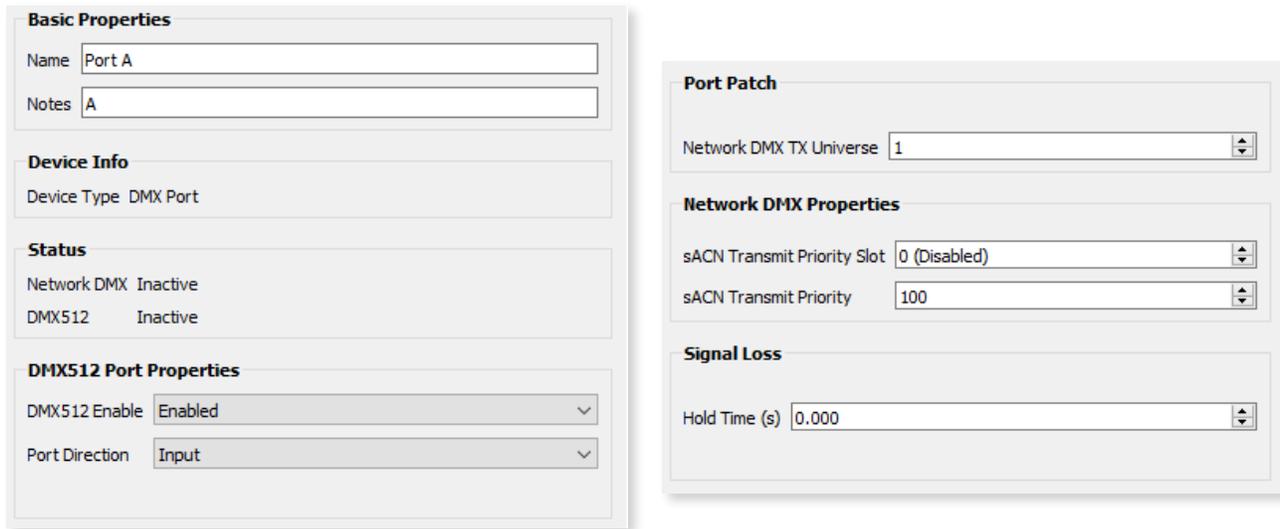
RDM PAUSE

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.

TIME SINCE LAST DISCOVERY

Will show the amount of time elapsed since the last RDM_GET commands were sent on this port. Read-only.

INPUT PORT PROPERTIES



BASIC PROPERTIES



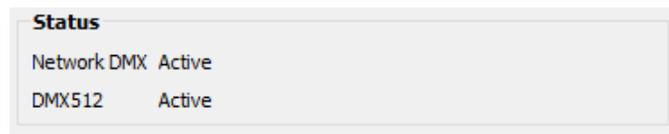
SUBDEVICE NAME

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



The **DMX512 Port Properties** window contains two dropdown menus. The first is labeled "DMX512 Enable" and is currently set to "Enabled". The second is labeled "Port Direction" and is currently set to "Input".

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.

PORT PATCH

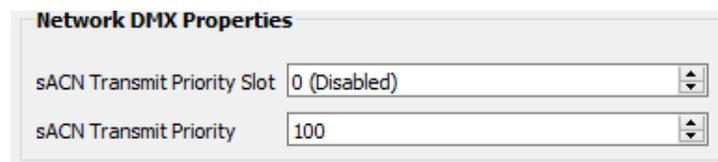


The **Port Patch** window contains a single dropdown menu labeled "Network DMX TX Universe" which is currently set to "1".

NETWORK DMX TX UNIVERSE

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

NETWORK DMX PROPERTIES



The **Network DMX Properties** window contains two dropdown menus. The first is labeled "sACN Transmit Priority Slot" and is currently set to "0 (Disabled)". The second is labeled "sACN Transmit Priority" and is currently set to "100".

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.

RDM PROPERTIES

Not applicable to Input Ports.

PATCHING PORTS

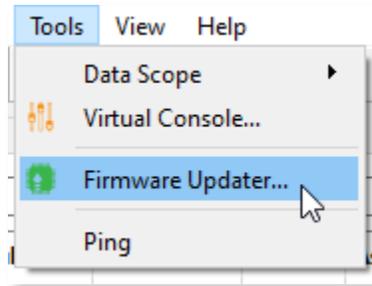
For in-depth instructions on patching the ports on your PWPP HH P1, refer to the **Pathscape manual** section titled **DMX Patch**.

UPDATING DEVICE FIRMWARE

Firmware updating may only be done using Pathscope.

The most recently released firmware is bundled with the most recent version of Pathscope. To ensure you have the most up-to-date firmware available for upgrading, ensure you have downloaded the most recent version of Pathscope 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 Pathscope, click the Tools menu, and select the  **Firmware Updater...** menu item.



This will bring up the Firmware Update window.

Status	Name	Type	IP Addr	Current	Latest	Selected	Message	Progress
Online	Light Panel PPWP DIN P2	Pathport 2-port DIN-mount	10.0.78.211	6.1.6	6.1.3		Latest version available is older than current.	
Online	NSB 4B3S3S	NSB PoE Wall Station	10.61.9.8	6.1.6	6.0.9.11		Latest version available is older than current.	
Online	NSB Gateway Slider Wall	Vignette 485 Wall Station		6.1.6			No firmware available	
Online	Rack PWPP DIN P1	Pathport 1-port DIN-mount / Pathport 1-port Wall-mount	10.4.194.20	6.1.6	6.1.3	<input checked="" type="checkbox"/>	Latest version available is older than current.	
Online	Rack PWPP DIN P2	Pathport 2-port DIN-mount	10.0.79.235	6.1.6	6.1.3		Latest version available is older than current.	
Online	Rack PWPP DIN P4	Pathport 4-port DIN-mount	10.1.143.13	6.1.6	6.1.3		Latest version available is older than current.	
Online	Rack PWPP RM P4	Pathport 4-port Rack-mount	10.1.139.227	6.1.6	6.1.3		Latest version available is older than current.	
Online	Rack PWPP RM P8	Pathport 8-port Rack-mount	10.6.27.72	6.1.6	6.1.3		Latest version available is older than current.	
Online	Rack PWPP WM P2	Pathport 2-port Wall-mount	10.0.32.189	6.1.6	6.1.3		Latest version available is older than current.	
Online	Rack VIA 5-Port DIN-mount	VIA 5-port with Fiber DIN-mount	10.30.132.148	3.9.0.0	3.9.0.0		Up to date.	
Online	Rack VIA 10-Port	VIA 10-port PoE Ethernet Switch	10.7.162.100	3.10.0.0	3.10.0		Up to date.	
Online	Rack VIA 12-Port PoE Switch	VIA 12-port PoE Ethernet Switch	10.7.201.142	3.10.0.0	3.10.0		Up to date.	
Online	Rack Vignette Clock	Vignette Clock	10.61.9.44	6.1.6	6.1.4		Latest version available is older than current.	

Select Latest
 Select Firmware
 Clear Selected

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.

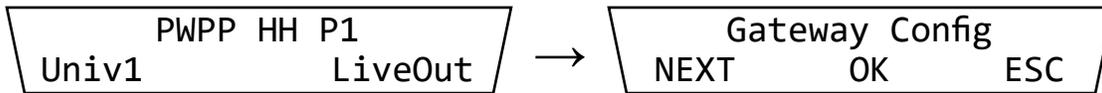
It is strongly recommended that you do not update VIA Switches and connected PoE devices at the same time. It is possible for the firmware update process to reboot the Switch before the data has finished writing to the PoE devices' memory. If the VIA Switch reboots at this point, the connected PoE devices' 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.

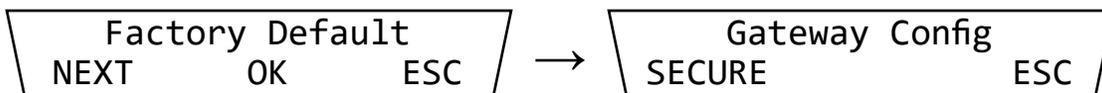
FACTORY DEFAULT

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

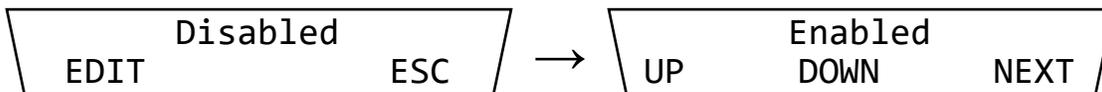
To factory default the PWPP HH P1, press any button twice to enter the main menu, which will show **Gateway Config** as the first menu item. Press the **OK** button to enter the menu.



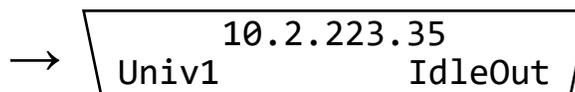
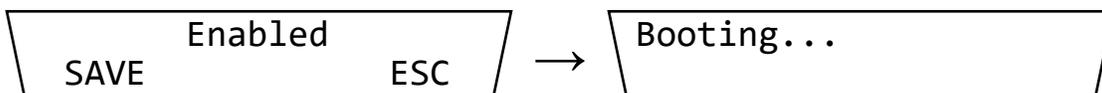
The first menu item in the **Gateway Config** menu is the **Factory Default** item. Press the **OK** button.



The next screen will show the current value for the property. You will need to change the value to “**Enabled**” to complete the Factory Default process. Press the **EDIT** button, and then press the **UP** or **DOWN** button to change the value to **Enabled**, then press the **NEXT** button.



Finally, on the next screen you must press the **SAVE** button to confirm. The device will then perform a factory default and will reboot itself. To cancel without performing a factory default, press the **ESC** button to cancel and return to the previous menu.



The device will then reboot, having reset itself to Factory settings. Note the device’s IP address will be reset to the default (starting with 10.x).

Before configuration can be restored, the unit’s Security Mode must be configured (add to a Security Domain, or enable Local Configuration Mode).

FRONT PANEL UI AND MENU

The PWPP HH P1 features a front panel UI, consisting of an LCD and three buttons 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 either add the PWPP HH P1 to a **Security Domain** using Pathscape, or if using Pathscape is not possible, you must select **Local Configuration Only** 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.

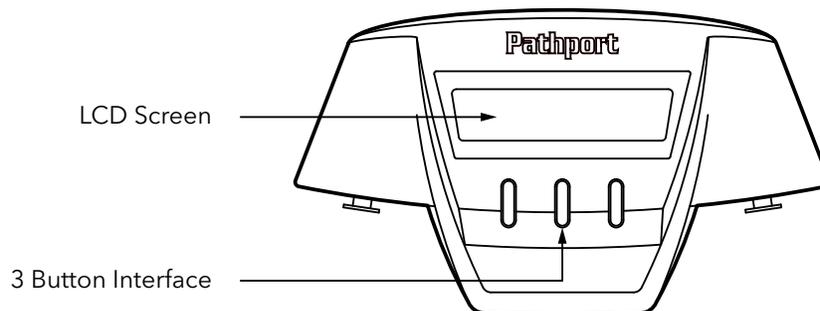
Non-standard Universes (Custom Patches) can only be edited and assigned to Ports using Pathscape.

If you must use the device without Pathscape, you must set it to **Local Configuration Only** 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

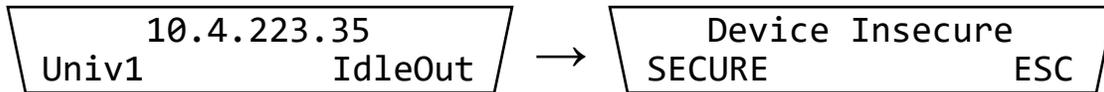
When the device boots up for the first time, or if it has been Factory Defaulted, you must choose a Security Mode.

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.**

OR:

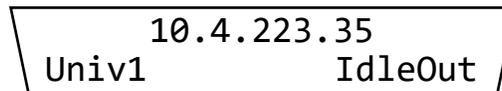
- Enable **Local Configuration Only** (Read only) mode.



- As described earlier in this manual, press any button twice to enter the menu, which will show the **Device Insecure** menu item. Press the left button to select **SECURE**. 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.

MAIN DISPLAY MESSAGES

When idle, the main LCD will show the device soft label (Name set in Pathscape), or its IP address if a Name has not been set.



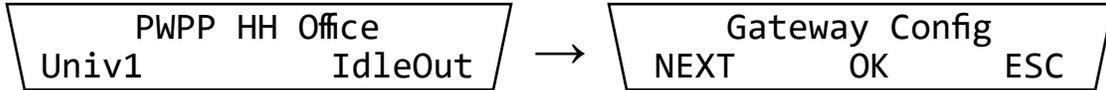
The lower line will show the Universe number (or patch name if using a custom patch), and the DMX status. The DMX status field will change depending if the DMX port is set as an input or an output, and if there is active DMX on the port.

The possible values for the DMX status are:

- **IdleOut:** DMX Port is set as an Output; DMX is not currently being output.
- **LiveOut:** DMX Port is set as an Output; DMX is actively being output.
- **IdleIn:** DMX Port is set as an Input; DMX is not currently being received.
- **LiveIn:** DMX Port is set as an Input; DMX is actively being received.

USING THE FRONT PANEL UI

With the main screen (above) showing on the LCD, press any of the buttons twice. The first button press will illuminate the backlight, while the second press will enter the main menu. The first menu item shown is the **Gateway Config** menu.



Press the **NEXT** button to cycle through menu items. Press the **OK** button to enter the currently displayed menu item to either enter a submenu or edit a property value.

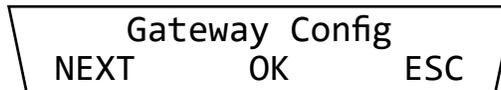
Press the **ESC** button to return to the previous/higher-level menu. Keep pressing the **ESC** button to exit out of the menu entirely and return to the main screen.

To edit property values, press the **OK** button to begin editing that property. Press the **UP** or **DOWN** buttons to scroll through the options for that property, and then press the **NEXT** button. Finally, press the **SAVE** button to accept any changes made, or press the **ESC** button to return without making changes.

The menu will time out after 30 seconds and return to the main screen, without saving any changes.

MENUS

GATEWAY CONFIG



This menu allows the user to Factory Default the device, allow the use of Unsecured RX protocols, setting the Network DMX TX Protocol, and setting which RX Protocols to receive (Pathport, ShowNet, ETC Net2, Art-Net, E1.31 sACN, and Pathway ssACN).

Menu Item	Description
Factory Default	Returns to the device to factory settings. Disabled (default): Factory Default will not be performed Enabled: After saving this property, the device will be reset to factory settings.
Allow UnsecureRX	Allows receiving of unsecured Network DMX Protocols. Disabled (default): Unsecured Network Protocols are not allowed. Accept Risk: After saving this property, Unsecured Network Protocols are allowed. Once saved, this property will be shown as Enabled .

Menu Item	Description
TX Protocol	Select the Network DMX protocol the PWPP HH P1 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
Pathport RX	Enable or Disable (default) the receiving of Pathport Protocol. If Allow UnsecureRX is Disabled, enabling this will have no effect.
ShowNet RX	Enable or Disable (default) the receiving of Strand ShowNet. If Allow UnsecureRX is Disabled, enabling this will have no effect.
ETC Net2 RX	Enable or Disable (default) the receiving of Strand ShowNet. If Allow UnsecureRX is Disabled, enabling this will have no effect.
Art-Net RX	Enable or Disable (default) the receiving of Art-Net. If Allow UnsecureRX is Disabled, enabling this will have no effect.
E1.31 sACN RX	Enable or Disable (default) the receiving of E1.31 sACN. If Allow UnsecureRX is Disabled, enabling this will have no effect.
Pathway ssACN RX:	Enable (default) or Disable receiving of Pathway ssACN.

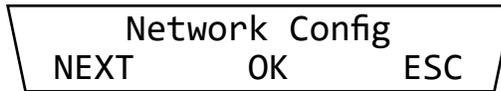
PORT CONFIG



This menu allows the user to configure the DMX port direction, Universe or patch, and DMX speed.

Menu Item	Description
Port Direction	<p>Set the DMX direction for the DMX Port.</p> <p>Choose DMX Input or DMX Output (default).</p>
Patch/Universe	<p>Allows selection of the patch for the DMX Port.</p> <p>Use the UP and DOWN buttons to scroll the list to choose from standard Universes, from 1 to 63999. Complex or custom patches that include merging and/or prioritization can only be set using Pathscape.</p> <p>For Output Ports: If you have previously set a Custom Output Patch using Pathscape, its name will be shown here as "Custom: <patch name>". Note the custom patch name may be truncated due to the character limit on the LCD.</p> <p>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.</p>
DMX Speed:	<p>Set the DMX Output speed. This has no effect on Input Ports.</p> <p>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.</p> <p>Slow: 20 packets per second (pps) Medium: 37 pps Fast: 40 pps Maximum: 43 pps (Default)</p> <p><Back>: Return to previous menu.</p>

NETWORK CONFIG



This menu allows the user to configure the IP Address, Subnet Mask and Gateway settings for the device.

Menu Item	Description
IP Address	Manually sets IP address (IPv4). Use UP and DOWN buttons to edit each octet. Currently selected octet will flash. Press NEXT button to move to next octet. After setting the last octet, press NEXT again to SAVE changes, or ESC to cancel.
Subnet Mask	Set subnet mask for the device. Use UP and DOWN buttons to edit each octet. Currently selected octet will flash. Press NEXT button to move to next octet. After setting the last octet, press NEXT again to SAVE changes, or ESC to cancel.
Gateway	Set default gateway for the device. Use UP and DOWN buttons to edit each octet. Currently selected octet will flash. Press NEXT button to move to next octet. After setting the last octet, press NEXT again to SAVE changes, or ESC to cancel.

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.

DMX PORT MONITOR



This menu item reports DMX input or output levels (depending on the port direction setting).

The top line of the display shows a starting slot number, then four DMX levels. The DMX level closest to the slot number corresponds to that slot number. Level information is shown as a percentage.



In the example above, the 1: corresponds to DMX Slot 1, which is at 50 percent (8-bit value 128); slot 2 is 75 percent (8-bit value 192), slot 3 is at 0, and slot 4 is at 50 percent (8-bit value 128).

Pressing the **UP** or **DOWN** button will move the starting slot number by 1 in either direction.

For example, pressing the **UP** button once will move the starting slot to 2, which will move the displayed DMX levels to the left.

```

  2: 75 00 50 00
UP      DOWN      ESC
  
```

Here, slot 2 is the first slot (at 75%), followed by slots 3 (at zero), 4 (at 50%) and 5 (at zero).

Press the **UP** or **DOWN** button to view relevant DMX slots. Slots past 512 will be shown as dashes "--", indicating there is no data to display.

```

  512: 00 -- -- --
NEXT      OK      ESC
  
```

If attempting to use DMX Port Monitor when the port is not active, the message "**Port Inactive**" will appear.

RDM TOOLS

This menu is only available when the DMX port is configured as an **output**.

```

      RDM Tools
NEXT      OK      ESC
  
```

Upon entering this menu, you will be presented with one option:

```

      RDM Devices
Find      ESC
  
```

Press the **FIND** button to begin discovery of RDM-enabled devices connected to the DMX port. Once discovery is complete, the total number of devices found will be reported.

```

      RDM Devices
      2 Found
  
```

If no devices are discovered, the message "None found" will be shown.

```

      RDM Devices
None found
  
```

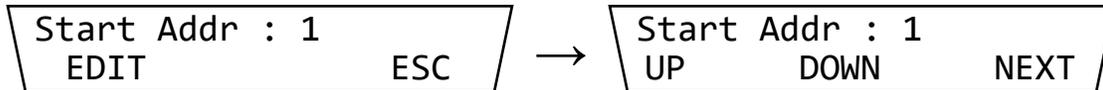
After 3 seconds, the device with the lowest serial number will be displayed. The device appears on the upper line of the display and with a 4-digit manufacturer identifier, followed by the serial number.

```

  5043:00001ee6
NEXT      ID      ESC
  
```

For a comprehensive list of manufacturer identifiers and corresponding company names, visit https://tsp.esta.org/tsp/working_groups/CP/mfctrIDs.php

Pressing the middle **ID** button will cause the device to start its identify behavior (typically, an indicator LED or LCD will flash), and will display the device's DMX start address. Press **EDIT** to change its start address.



Use the **UP** or **DOWN** buttons to change the DMX start address of the device, and pressing **NEXT** allows the new address to be saved. Once saved, press **ESC** to return to the device list.

To cycle to the next RDM device, press the **NEXT** button and repeat the above steps to edit the DMX start address if needed.

TEST DMX OUTPUT

This menu is only available when the DMX port is configured as an **output**. Use this menu to test the DMX output of your network on one or all slots in the currently configured output Universe.



Press **OK** to enter the menu. The next screen will show “**Chan**” with a flashing “**1**”.



Use the **UP** or **DOWN** buttons to select the desired DMX slot to test. To select ALL slots, press **DOWN** once. “Chan All” will be shown. Press **NEXT**.



“Lev 0” will then appear, indicating **DMX Level**. Press and hold the **UP** button to increase the DMX level for the selected slot(s). The longer you hold the button, the faster the level will ramp up. Release the button to stop at the current value.



Once the level reaches 255, continuing to press or hold UP will drop to zero and then begin ramping up again.

Pressing the **FADE** button will cause the gateway to automatically fade the selected slot from zero to full, then back down to zero again. Press the **STOP** button to stop the fade at the current DMX level, at which point you may press FADE again to resume, or press UP to ramp up manually.



The **FADE** function will continue fading the DMX slot level up and down until the user presses **STOP**, **ESC** or the 30-second timeout expires.

APPENDIX 1: ELECTRICAL, COMPLIANCE & OTHER INFORMATION

ELECTRICAL INFORMATION

- Power input:
 - Power-over-Ethernet (PoE): Class 1 Device, 4W Maximum draw
 - Auxiliary power: included 9V battery; for configuration only - device will go to sleep after short time without user input.
- DMX Ports:
 - 60V fault protection on DMX port

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

PHYSICAL

- Weight: 0.68 lbs (0.31 kg) [with hanging bracket installed]
- Dimensions: 5.95" W x 3.4" H x 1.88" D (218mm W x 43mm H x 47.8mm D) [base device, without attached hanging bracket]
- Dimensions: 5.95" W x 3.4" H x 3.87" D (218mm W x 43mm H x 98.3mm D) [base device, with attached hanging bracket]