eLink LIGHTING PROTOCOL ROUTER

Model PWELINK RM P2 RJ45EC REAR

User Guide

December 2021

Pathway® Connectivity Solutions

Pathway Connectivity | #103 - 1439 17th Ave SE Calgary, AB Canada T2G 1J9
Phone: + 1 866 617 3074

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 secure access to your network, both physically and technologically. To continue, you must acknowledge that you have read this statement and accept these risks.

CONTENTS

ABOUT eLink LIGHTING PROTOCOL ROUTER

The **Pathway eLink™** Lighting Protocol Router is designed for entertainment DMX-over-Ethernet systems. This manual covers the model **PWELINK RM P2 RJ45EC REAR**.

The eLink Lighting Protocol Router is intended specifically for signal routing between distinct Local Area Networks, while maintaining security and isolation between them. The eLink is able to convert between several popular DMX-over-Ethernet protocols, including **Pathport Protocol, sACN (E1.31)**, **Art-Net**, **Strand ShowNet**, and **Pathway ssACN (Secure sACN).** The eLink can also optionally loop back converted protocols on a single network, when physical isolation of data is not needed.

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

PHILOSOPHY

When you have two distinct networks and need to get data from one to the other, a simple solution is to connect them together with a switch. However, by doing this you no longer have two separate networks, but one larger network in which all multi-cast and broadcast data is present everywhere. This is almost always a bad idea. Care should be taken to avoid conflating traffic.

When using the eLink to connect the two networks, it acts as an Entertainment Lighting Protocol traffic cop. **Only the protocols, universes and slots you define are allowed to pass from one system to the other**.

At its simplest, eLink is like having a network switch and four Pathport 8-port DMX/RDM Ethernet Gateways compressed into a compact 1/2 rack unit. The eLink supports 16 Data Paths, and five different entertainment lighting protocols simultaneously, each having priority rules to merge up to 128 sources in real-time.

Use Pathscape to create custom patches defining any data slot at any priority on one or more supported protocols to be output at a different priority or protocol on either of its two Network Interface Cards (NICs). You can monitor a specific slot on the control console to change priorities on the fly.

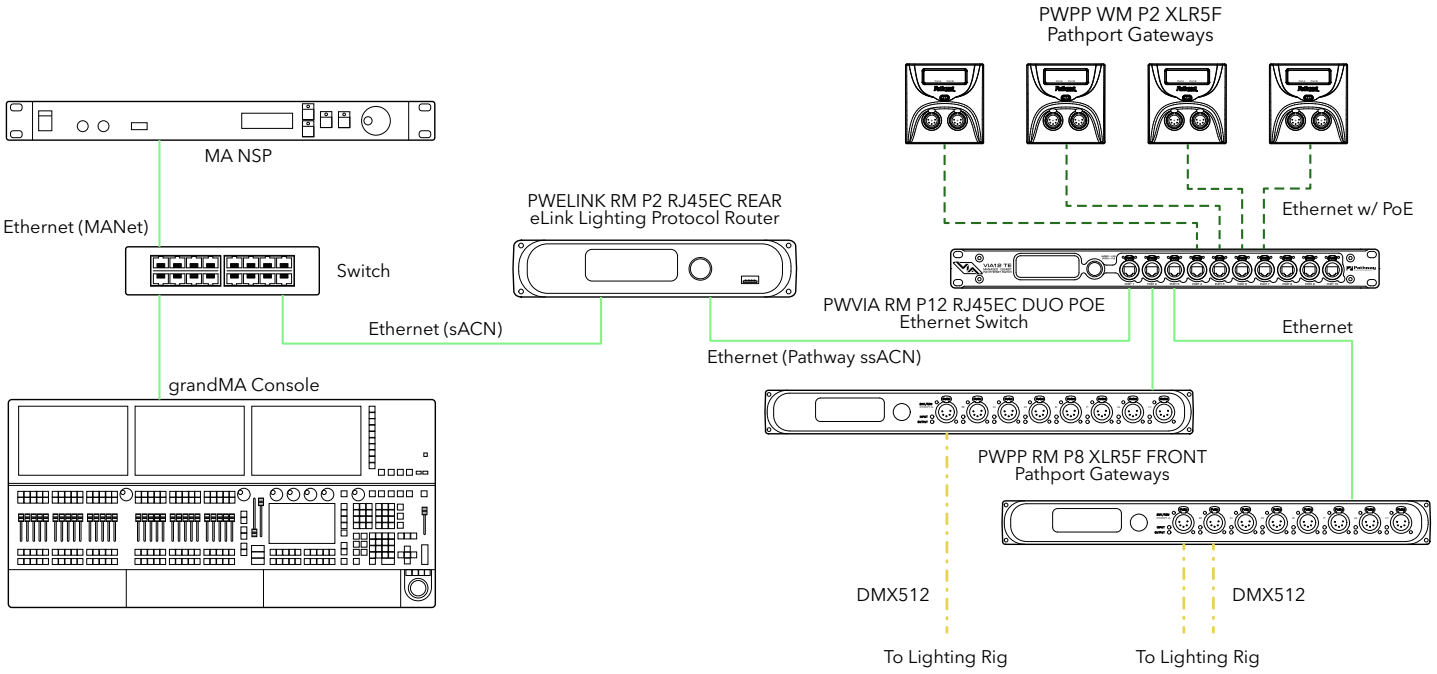
The eLink aids in enforcing good networking practices, making your networks cleaner, faster and more reliable.

APPLICATIONS

GUEST CONSOLE ON-RAMP

Every day, Performing Arts Centers host touring companies that bring much of their own kit, but within the venue is much of the fundamental infrastructure needed to maintain comfort and safety of the patrons. If the permanently installed house lighting system resides within its own Security Domain, it's desirable to open up only a few channels for the touring act to run the auditorium lighting.

Using a custom patch on the eLink, you can allow a large and complex system to be simplified down to just a few channels the touring programming can patch. This ensures that regardless of the patch in the guest console, your system maintains its independence and integrity.



Example of a network using the Guest On-Ramp application. Note the MANet data never reaches the downstream system.

CONSOLE ON/OFF SWITCH

eLink features a Contact Closure Input that can be configured to hold or kill any or all Data Paths. With one switch, you can cut off a touring control system during mandated break times or during emergency situations.

CONNECTING A BUILDING AUTOMATION SYSTEM TO AN ARCHITECTURAL FACADE

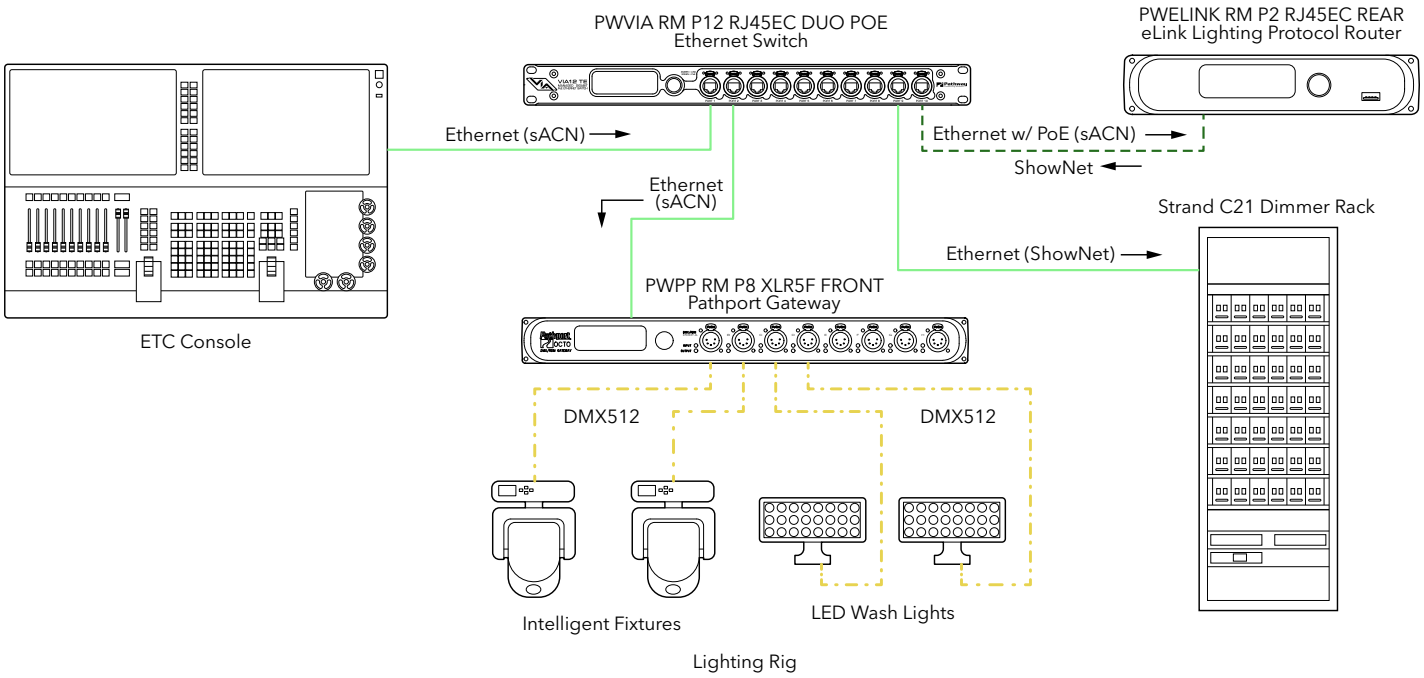
Large building and public spaces use Building Automation Systems that often need to interact with or are connected to the building IT network. These spaces typically have an external architectural facade that is treated with dynamic LED lighting.

Although the lighting looks can be triggered by the BAS, it's desirable to maintain two separate networks. In such a situation, an eLink can route the triggers from the building to the solitary entertainment network without introducing sensitive or life safety system traffic.

SIMPLE REAL-TIME PROTOCOL CONVERSION ON ONE LAN WITH LOOPBACK

On a simple, small LAN where network isolation is not important, you can configure eLink to output converted protocols back out on the primary NIC. This may be desired in a system with, for example, a C21 dimmer rack.

The console can be outputting sACN to the entire network. Place the eLink on that network and configure it to convert sACN to ShowNet and output back onto the same network. The C21 rack can then coexist on the same network as everything else, and receive only the ShowNet protocol. Everything else receives sACN and ignores ShowNet.



Example of a network transmitting converted protocols back onto the primary NIC for integrating a C21 dimmer rack into an sACN system

SixEye NETWORK MONITOR

Like many of Pathway Connectivity's products, eLink is fully supported by the Six cloud management software.

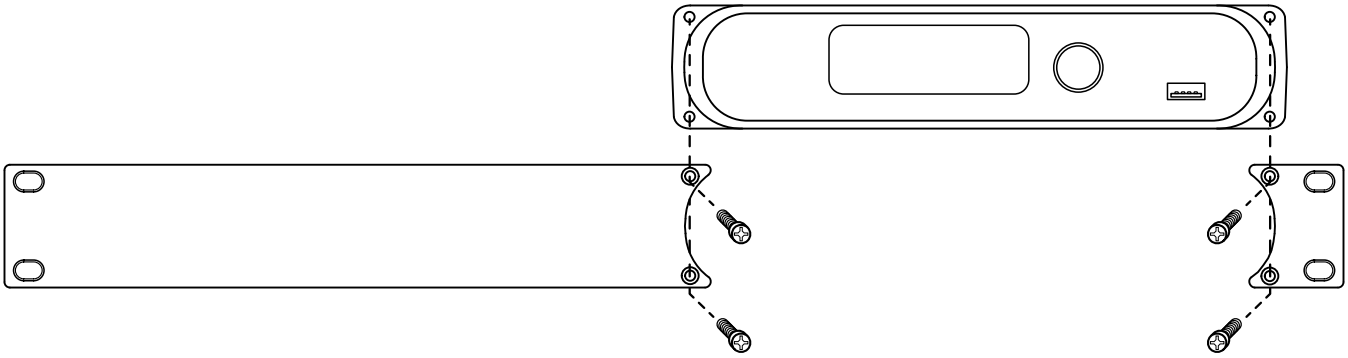
Drop an eLink on any entertainment system and securely control the flow of data or monitor DMX levels from anywhere in the world, using a computer or smartphone.

INSTALLATION INSTRUCTIONS

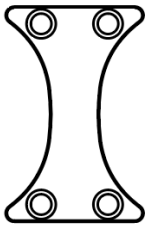
The eLink Lighting Protocol Router is intended for desktop use, or to be mounted in a standard 19” equipment rack, using the included rack ear accessories.

Rack ear accessories for installing the eLink unit to 19” equipment rack. Long and short sections can be swapped to either side as needed.

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



If mounting two eLink units together (or an eLink and a Pathport Rack-mount 4-Port Gateway) use the rack ear coupler between the units to fit both into one rack space.

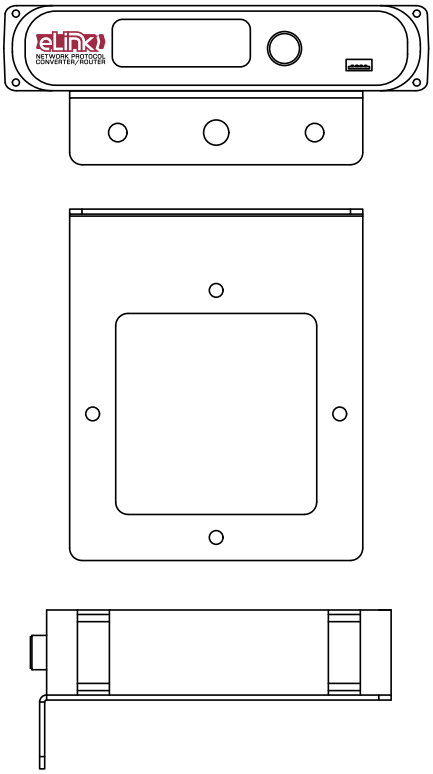


Rack ear coupler included with the eLink for attaching unit to another eLink or Pathport Rack-mount 4-Port Gateway in a 19” equipment rack

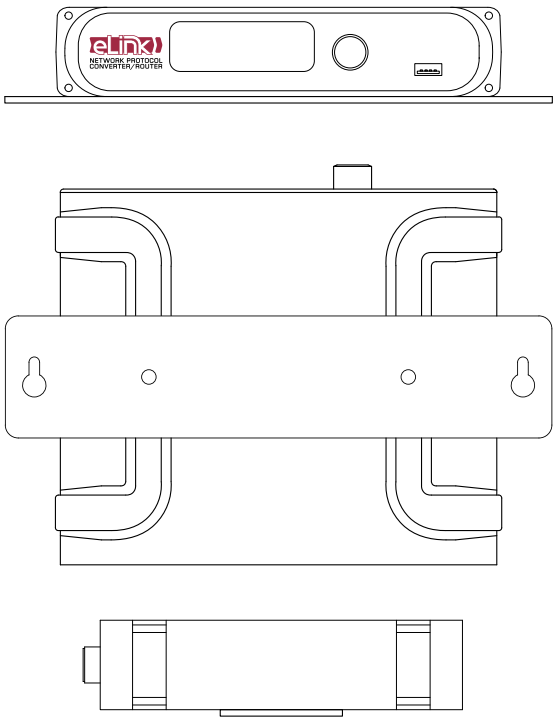
If using the eLink on a desktop permanently, you may wish to apply the adhesive rubber feet pads to the bottom of the unit. Simply peel them off the adhesive backing and apply to the bottom of the metal enclosure, with one on each corner.

OPTIONAL MOUNTING ACCESSORIES

Truss-mount adapters (PWACC TMSM) and wall-mount kits (PWACC WMSM) are available as accessories.



PWACC TMSM Truss-mount Kit



PWACC WMSM Wall-mount Kit

INSTALLATION ENVIRONMENT

The eLink Lighting Protocol Router is intended for installation in a dry, indoor location. Ambient operating conditions are **32°F to 122°F (0°C to 50°C); 5-95% relative humidity, non-condensing.**

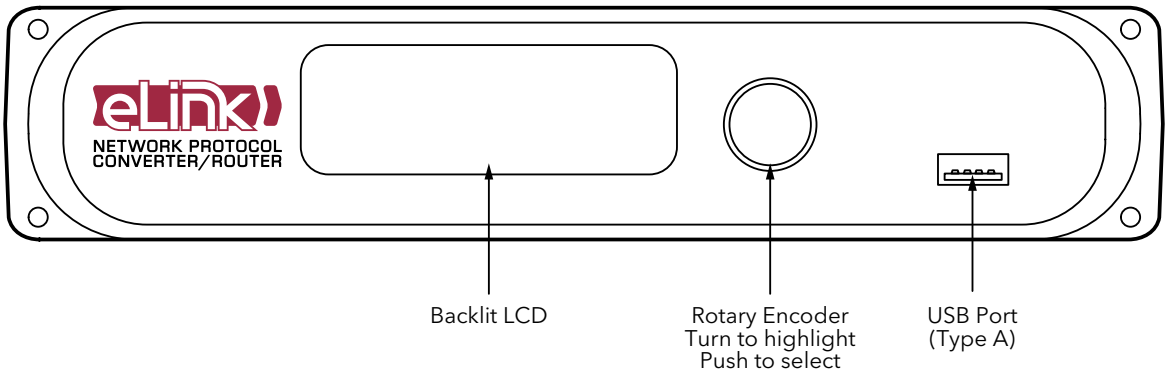
Warning: If using a 24-48VDC power supply, its AC socket outlet shall be installed near the equipment and shall be easily accessible.

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

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

PANEL LAYOUTS

FRONT PANEL



LCD

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

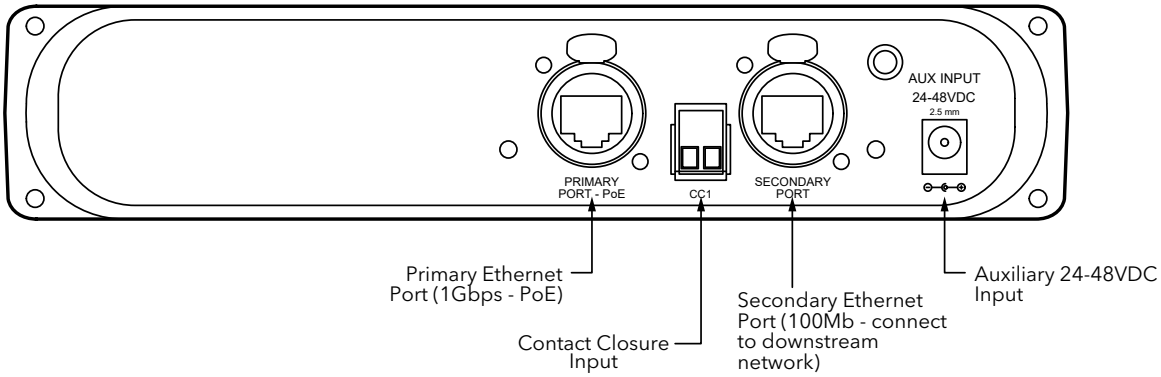
ROTARY ENCODER

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

USB PORT

USB Port (Type A) for future use. Does **not** support USB peripherals (keyboards, mice, etc).

REAR PANEL



etherCON PORTS

The eLink has two RJ45 etherCON ports on the rear of the device: the Primary Port, and Secondary Port. The Primary Port should be connected to the main/source network (and PoE source). The Secondary Port should be connected to the downstream network.

Each etherCON port has a status LED: to the left of the Primary Port, and to the right of the Secondary Port. The LEDs will light up amber when a link is established, and will flash when there is network activity. If the LEDs are off, there is no active link.

CCI (CONTACT CLOSURE INPUT)

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

POWER CONNECTIONS

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

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

CONFIGURATION

The eLink Lighting Protocol Router may be configured from the front panel interface using the LCD and rotary pushbutton encoder. However, we recommend using our free software tool, Pathscape. To download Pathscape, visit the Pathway website at https://www.pathwayconnect.com.

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

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

SECURITY

BACKGROUND INFORMATION

On **January 1, 2020**, California will be 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 Security** below) or requires the users to change the password before being able to use it (See **Creating a Security Domain** below). With Pathscape V3, we provide features that protect our products from unauthorized access or use by enforcing passwords. Furthermore, 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. As of 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.

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 recommend writing down and storing the password for any such devices.

5. Products that are fully configurable from the front panel can create their own unique password. Only with network configured products will you need to type a password; one password for all devices on 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.

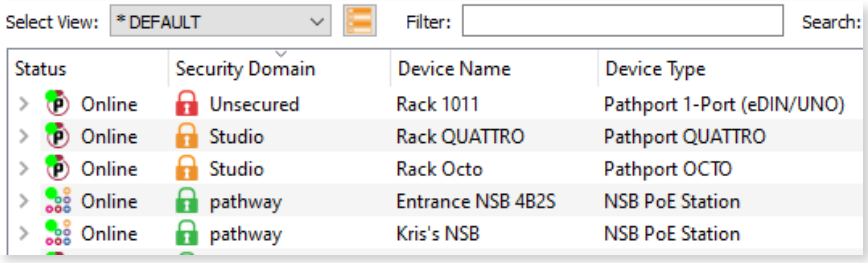
8. The complete network configuration may be saved without a password before factory defaulting devices. Applying the saved configuration will require a new password to be set for the network.

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.

10. Pathway does not store personal information such as names or email addresses on our devices.

SECURITY DOMAINS

To simplify the process of managing security on your network, Pathscape (beginning with version 3.0) introduces the concept of a "**Security Domain**". Below we will describe how to create a Security Domain and add or remove devices from it. In the **Device** tab of Pathscape there is a new view that shows you the name of the device's domain and a **padlock icon** showing its current state.



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

RED PADLOCK - Unsecured Device

Any device shipped after **January 1, 2020** will have version 5 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 - Secured Device not in the Current Domain

Devices that have been added to a security domain will appear with an amber padlock. These firmware v5 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 - Locally Secured

You may also see **Locally Secured** beside an amber padlock. Locally Secured means the front panel was used to create a unique (and hidden) password to allow front-panel-only configuration. To gain read/write privileges with Pathscape, you **must factory default the device** from the front panel and add it to the local security domain using Pathscape.

GREEN PADLOCK - Secured Device in Current Domain

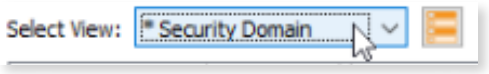
Once you have logged into a Security Domain with a password, any device in your domain will appear with a green padlock and all their properties will be Read/Writable.

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

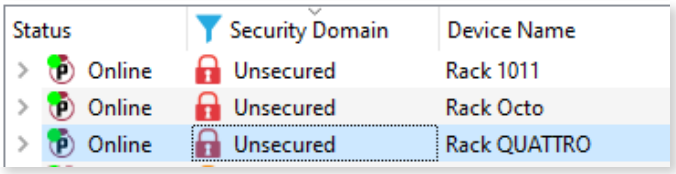
If the Security Domain cell is empty, this device is using Version 4 firmware and cannot be secured. Pathscape 3 will be able to read and write properties exactly like Pathscape 2. If you upgrade to v5 firmware the device will appear with a red padlock and you will need to add it to a domain before you can use it.

CREATING A SECURITY DOMAIN

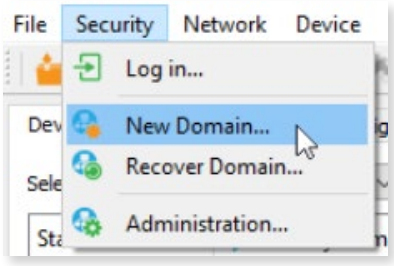
- After starting Pathscape, the online devices will populate the Device View.
- Choose the **Security Domain** view from the **Select View** dropdown

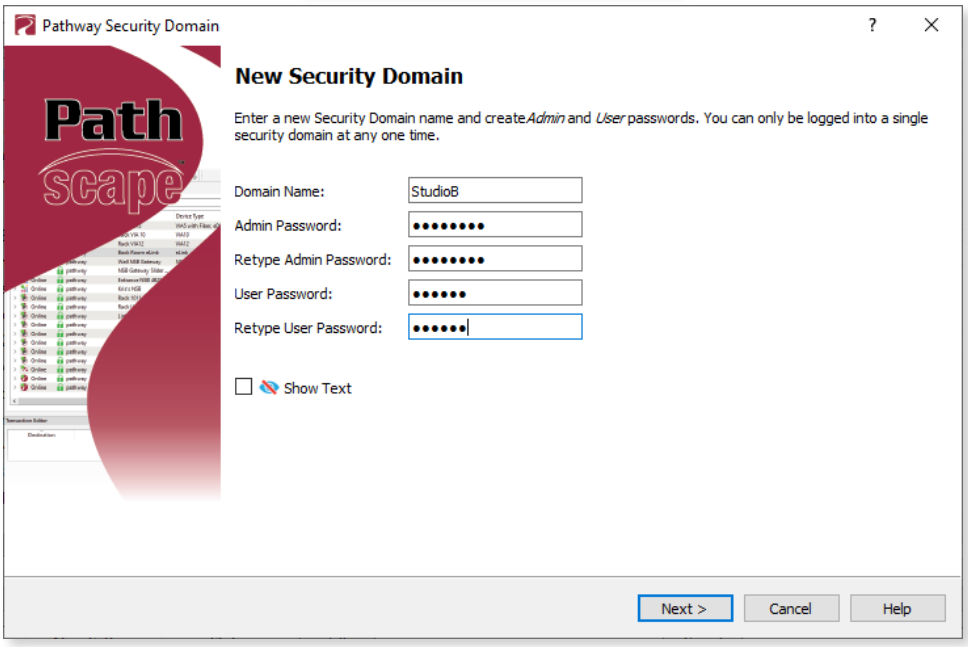


- Each device running V5 or later firmware will have a **Red "Unsecured"** value in the **Security Domain** column.



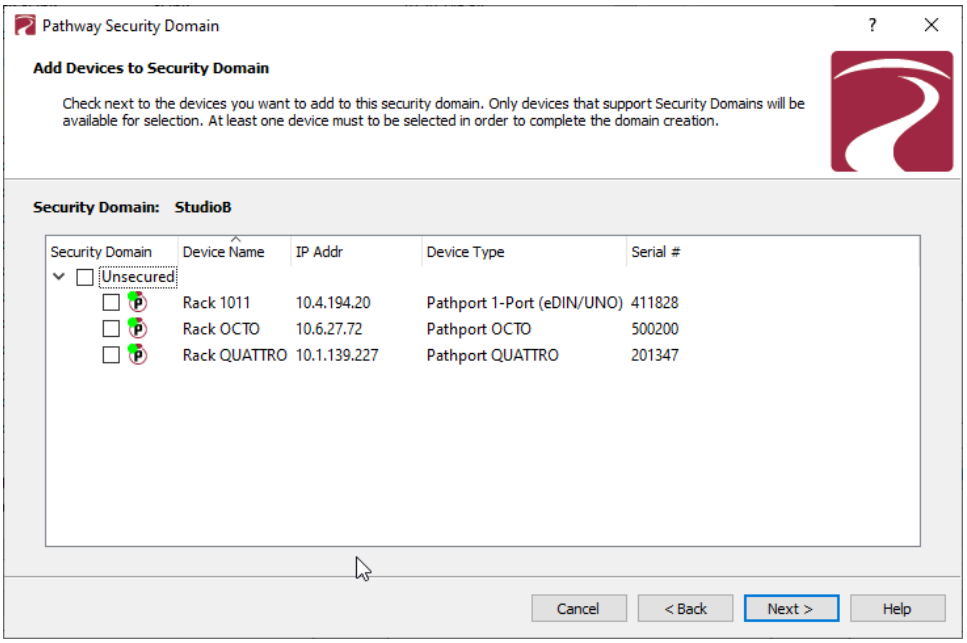
- (Optional) You may update devices to current firmware by going to the **Tools** menu and selecting **Firmware Updater**. Select the devices to upgrade, and choose **Select Latest**, then **Send Firmware**. (See the **Upgrading Device Firmware** section for more detail). The devices will go offline and come back with a **red padlock**.
- From the **Security** menu, choose **New Domain.**





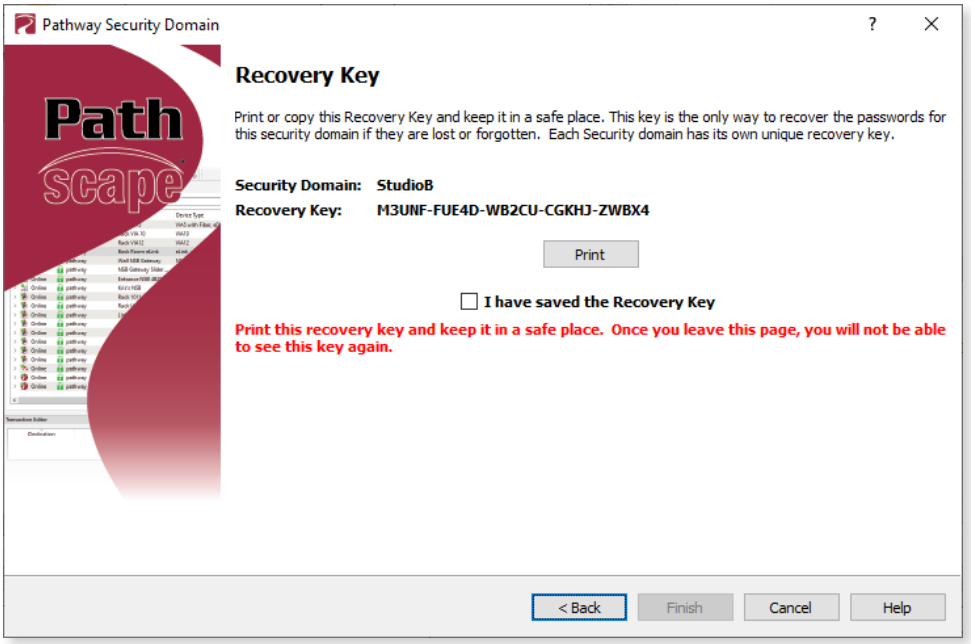
- Enter the new **Domain Name** and **Administrator** and **User passwords**, then click **Next.**
  - The **Administrator** can change passwords, factory default devices and add or remove devices from the domain.
  - The **User** can change device properties and save and restore show files, but cannot change domain passwords, factory default devices or add/remove devices. There is one User account password for all users.

- Add all the Unsecured devices on your network by checking the top checkbox labeled "**Unsecured**" 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 Continue.

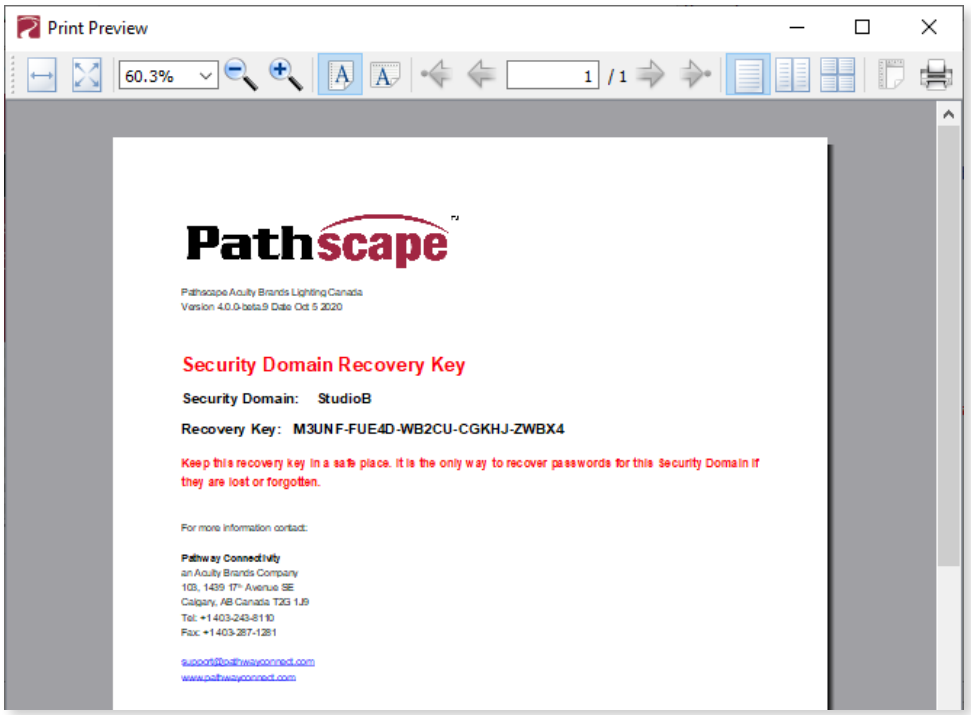


- The next window will show the **Recovery Key**. This key will allow you to recover Security Domain access should the passwords be lost or forgotten.

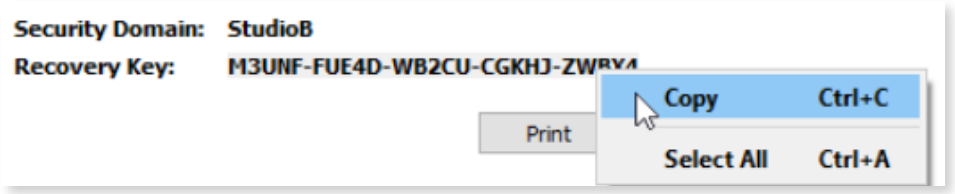
  It is extremely important to keep a record of this Recovery Key, as this is the only time it will be shown to you. Print the Recovery Key.



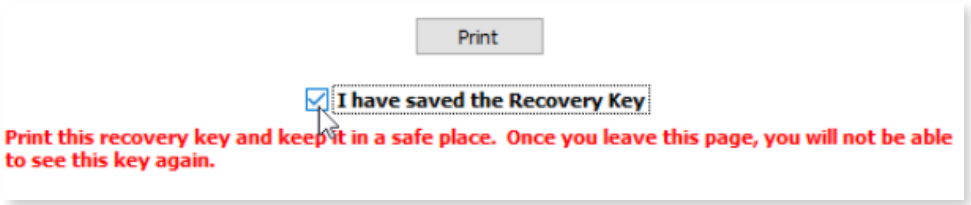
- Clicking the **Print** button will open a Print Dialog, from which you may choose a printer to print to.



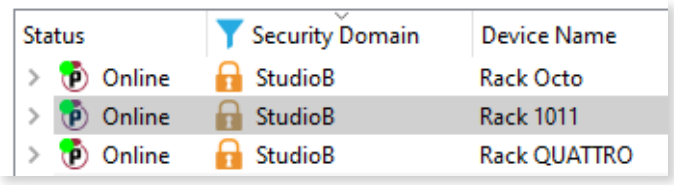
- You may also right-click on the Recovery Key, then **Select All** and **Copy** the key to the clipboard and store it in a safe place.



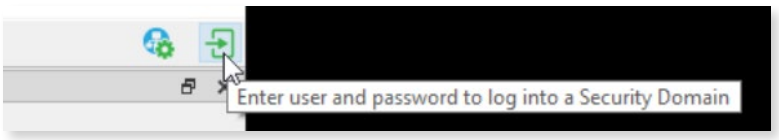
- In order to proceed, you **must click the checkbox** acknowledging you have printed or saved the Recovery Key in some way.



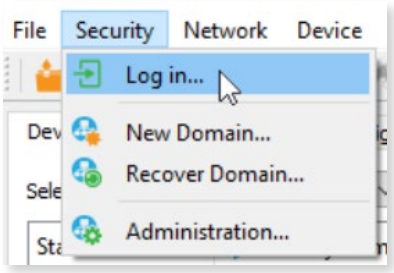
- Click **Finish** and the window will close, and the devices will be added to the domain. The devices will have an **amber padlock** and their properties will be read-only.



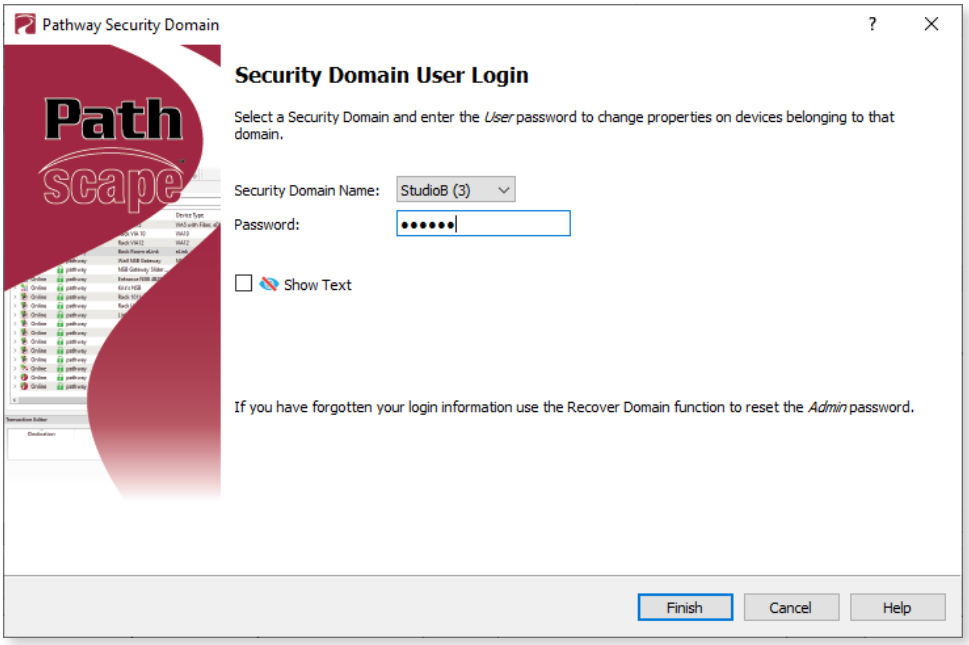
- To configure the devices, you must log in to the domain **as a user** by pressing the Log In button in the toolbar. **Note**: The **Security Toolbar** option under the **Window** menu must be checked



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

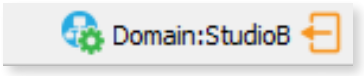


- Enter the **User** password for the Security Domain that was just created, and click **Finish**.



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

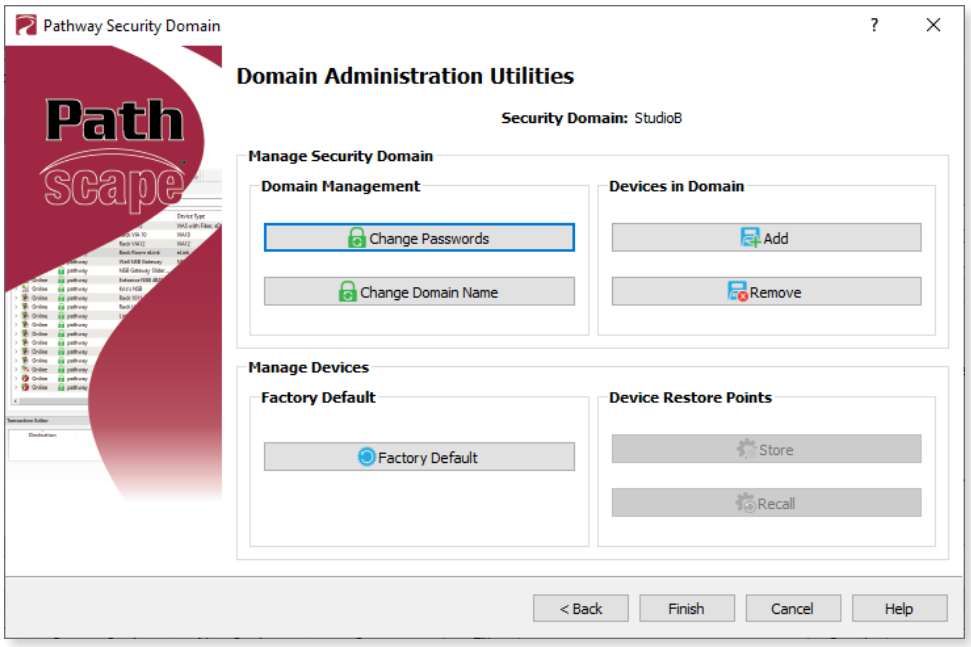
Once logged into a domain, the Log In button will change to the Log Out button, and the name of the domain currently logged into will appear next to it.



ADMINISTERING A DOMAIN

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

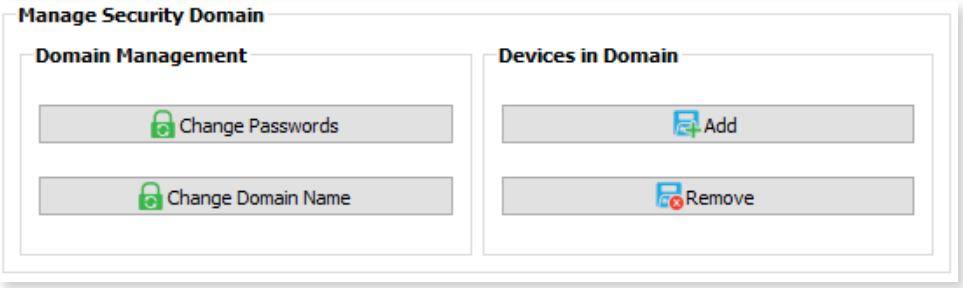
Enter the **Admin** password for the Security Domain, and the **Domain Administrator Utilities** window will appear.



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

MANAGE SECURITY DOMAIN

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



DOMAIN MANAGEMENT

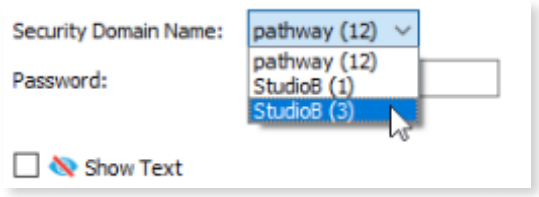
CHANGE PASSWORDS

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

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

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

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



You will have to remove the devices that are 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 name is the number of devices that are in that domain. This should 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 **Unsecured**. 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**.

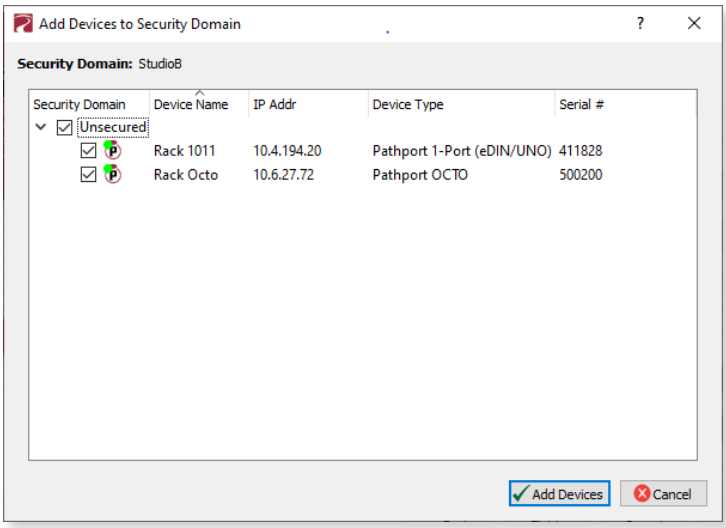
The window will close, and you will be logged out of the current domain, and the Domain Name will be changed to the new value. **You will have to log into the Domain again** to make any further changes.

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. It is advised to make note of the changed domain name and store it in the same location as the Recovery Key, so the domain can be recovered in the future if necessary.

DEVICES IN DOMAIN

ADD

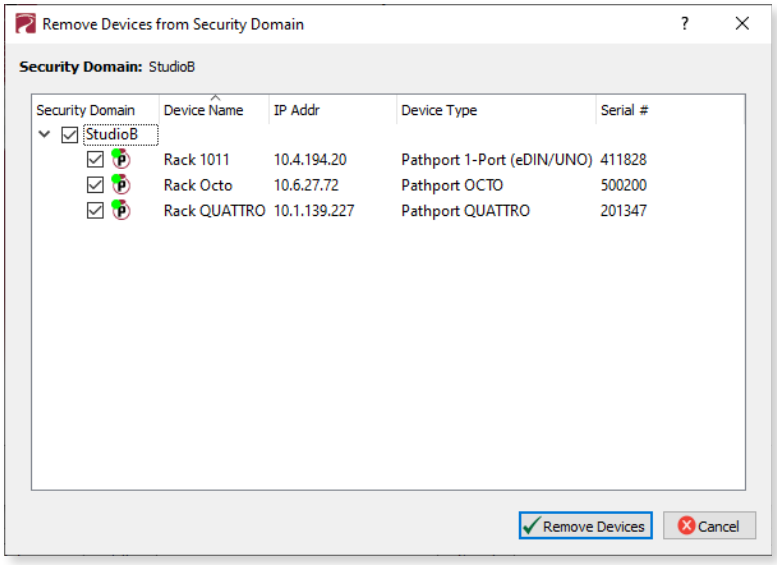
Clicking on this button will bring up the **Add Devices** window, where Unsecured devices can be added to the current Security Domain.



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 "Unsecured" which will auto-check all the devices' checkboxes.

REMOVE

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



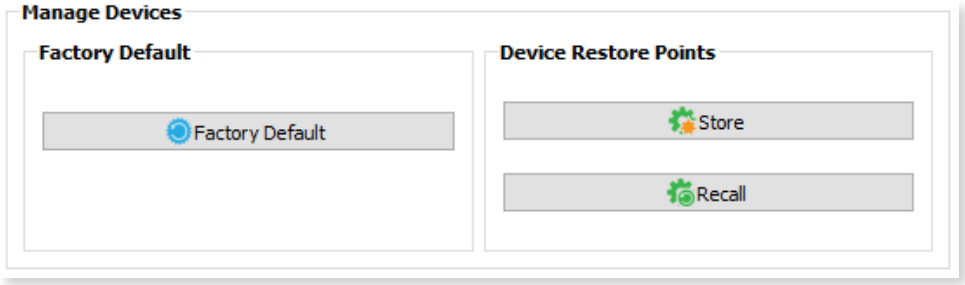
Click on the checkboxes next to the devices you want to remove from the Domain, and click the **Remove Devices** button. To remove all the listed devices, click the top checkbox next to the Domain Name which will auto-check all the devices' checkboxes.

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

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.

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**.



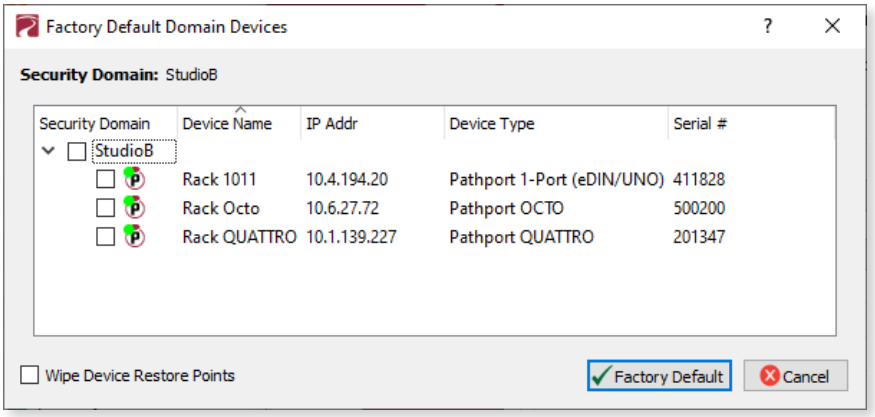
FACTORY DEFAULT

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 that you do not have a password for, you must have physical access to factory default them before you regain network configurability.

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



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

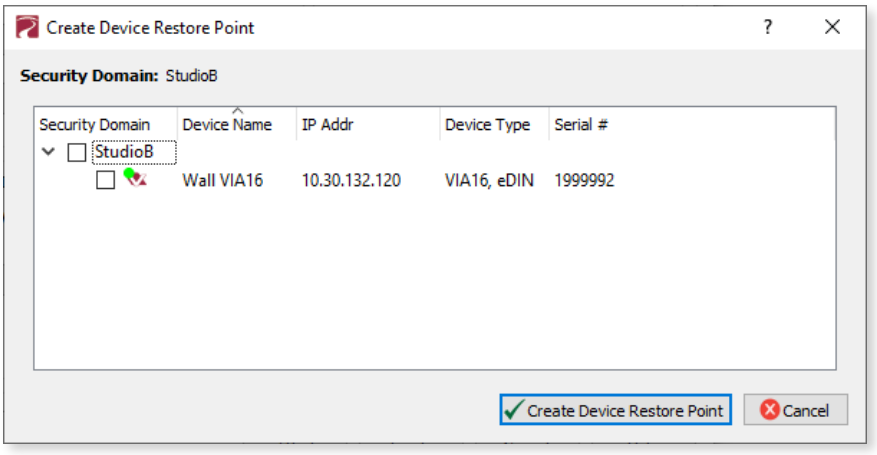
DEVICE RESTORE POINTS

With the release of firmware V6.0, certain Pathway products (new VIA Switches including models PWVIA RM P12; Pathport gateways including PWPP RM P8 & P4, PWPP DIN P4, and Vignette Clock) will support Device Restore Points.

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

STORE

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

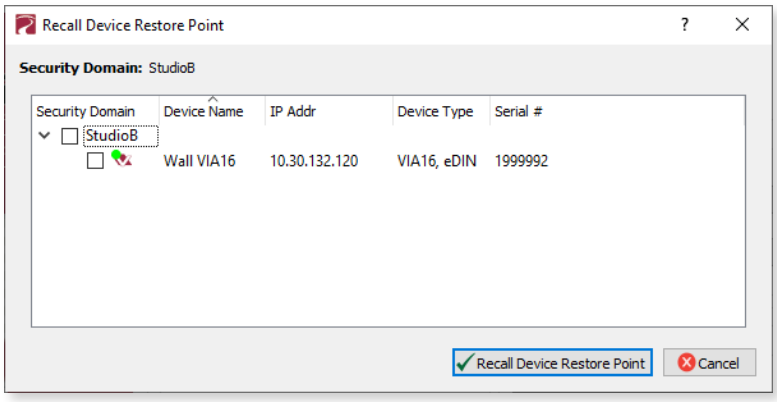


Click the checkbox next to each device on which you'd like to create a restore point. To check all devices, click the topmost checkbox. Click **Create Device Restore Point** to confirm.

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

RECALL

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



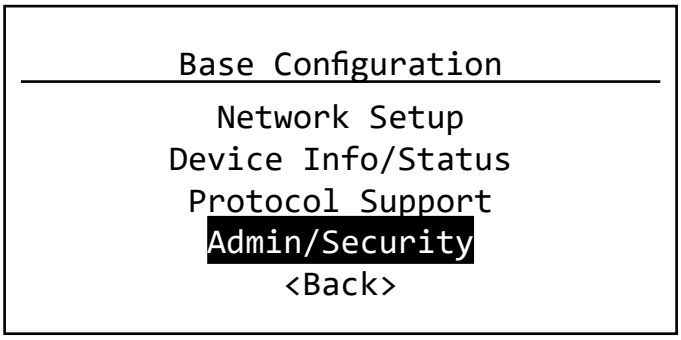
Click the checkbox next to each device on which you'd like to recall its restore point. To check all devices, click the topmost checkbox. Click **Recall Device Restore Point** to confirm.

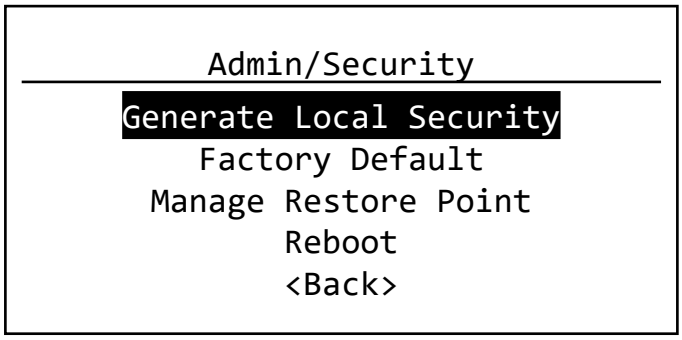
Note that if there are no connected devices that support this feature, this button will be grayed out.

LOCAL SECURITY - USING eLink WITHOUT PATHSCAPE

The eLink Lighting Protocol Router has features that use unsecured protocols. You may not intend to use Pathscape, but “bad actors” could potentially access the device and change the configuration. Therefore it is prudent to configure **Local Security** to protect your network if you want to use the eLink, but are not using Pathscape to add your devices to a **Security Domain**.

From the **Admin/Security** menu on the front panel, select **Generate Local Security**.



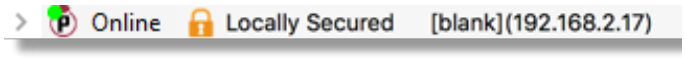


ONCE LOCAL SECURITY HAS BEEN GENERATED, THE eLink WILL BE CONFIGURABLE ONLY BY USING THE FRONT PANEL.

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 secure access to your network, both physically and technologically. To continue, you must acknowledge that you have read this statement and accept these risks.

If you do open Pathscape, this device will be part of the domain “Locally Secured”.



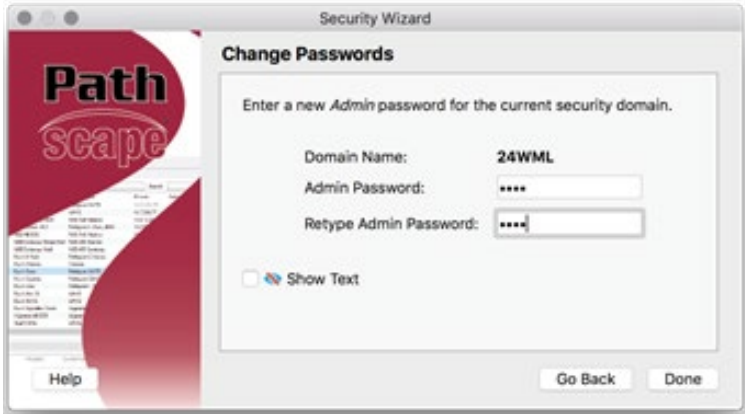
You cannot login to this security domain. If you want to now use Pathscape to configure this device, you must use the front panel to reset its Security Settings, then use Pathscape to add it to a Security Domain.

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**.

- Type in the 20-digit **Recovery Key** and press Continue.



- Type in a new **Administrator Password**.

- From the menu choose **Security > Administration** and Change Passwords to set a new User password.

RETAINING DEVICE SETTINGS FROM UNKNOWN DOMAINS

There are times when you don't know the password of a Security Domain, but you'd like to retain all its configuration. Without logging in to a Domain, all devices that appear with amber padlocks are read-only. If you save a show file, the configuration of all devices is saved. You can then factory default the devices using the prescribed method; see the Pathway website for a comprehensive document titled **Factory Defaulting Pathway Ethernet Devices**, describing how to manually factory default all our devices.

Once they reappear in Pathscape with a red padlock, add the devices to a Security Domain, then 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)**, you will not be able to configure them; **you must use Pathscape 3 or newer**. 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.

INTRODUCING PATHWAY ssACN (Secure sACN)

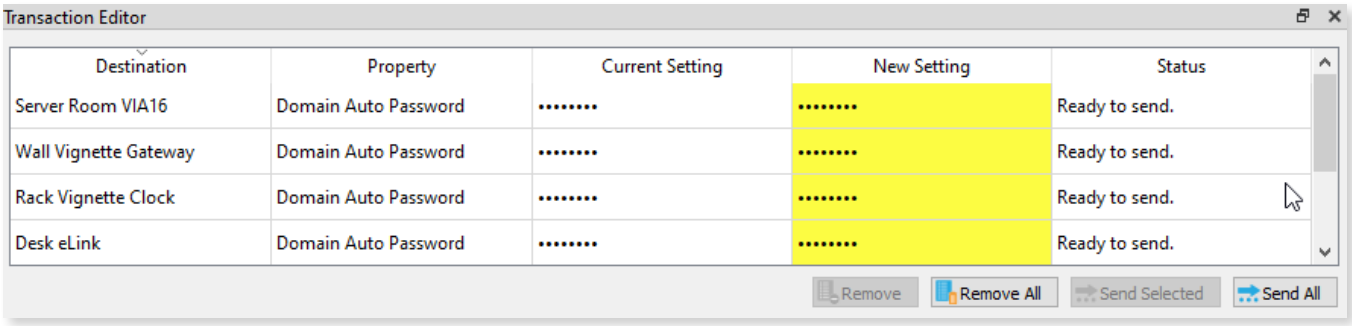
Pathway ssACN (Secure streaming ACN) is a new protocol developed by Pathway using much of ANSI E1.31, but adds a layer of authentication. This feature requires **device firmware version 6.0 or later**.

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.

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

DOMAIN AUTO ssACN PASSWORD

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



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

NOTE that the **Domain Auto** password is **NOT** the same as the **Domain** password. Recall that the Domain password is the 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:

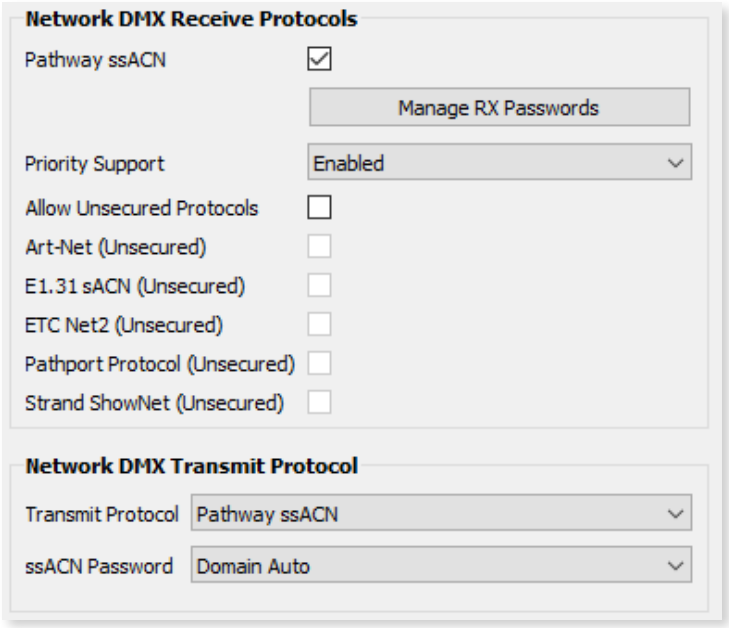
- **If you need to send DMX data across different Security Domains**: specify a custom **ssACN TX password**, and enter the same password on the receiving devices under **ssACN RX passwords**. The receiving devices will then be able to authenticate that data. Domain Auto passwords, as noted above, are 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.

CHOOSING PATHWAY ssACN AS NETWORK PROTOCOL

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

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

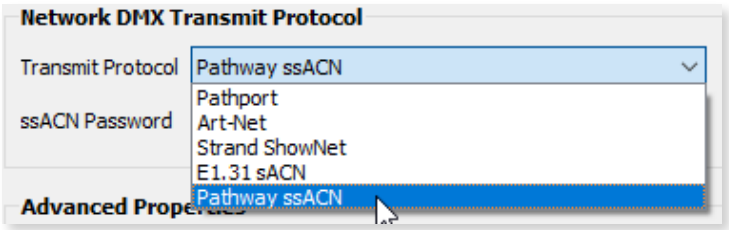


These are the same sections where you would specify your devices to use Network DMX protocols like E1.31 sACN or Art-Net, for example.

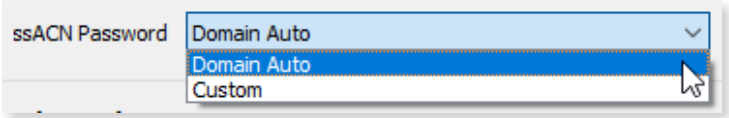
In the **Network DMX Receive Protocol** section, simply check the Pathway ssACN checkbox. We recommend unchecking the Allow Unsecured Protocols checkbox, if previously checked, since end devices can receive **both** ssACN and unsecured protocols if left checked.

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

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

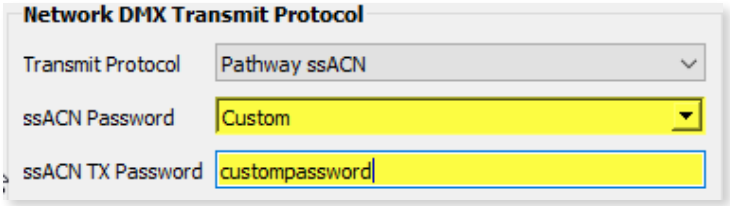


Once you select **Pathway ssACN**, the **ssACN Password** drop-down menu will appear.



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

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



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

More on managing ssACN Passwords below.

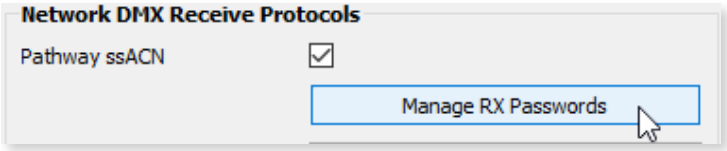
MANAGING PATHWAY ssACN PASSWORDS

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

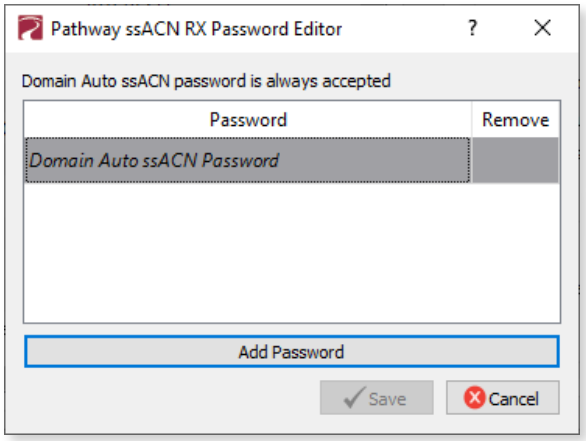
If you are using custom Pathway ssACN passwords, you will need to tell those devices transmitting Pathway ssACN what password to use, as well the devices that are receiving it what passwords to accept.

RX (RECEIVE) PASSWORDS

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

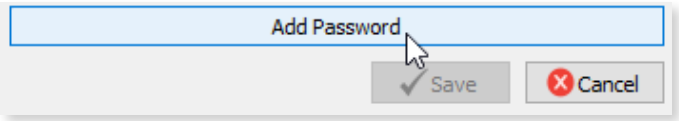


Click it to open the **Pathway ssACN RX Password Editor**.

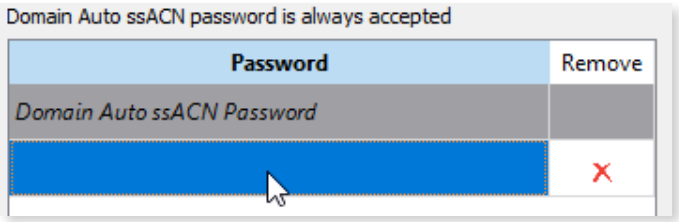


Use the Pathway ssACN RX Password Editor to add custom passwords the selected device should accept.

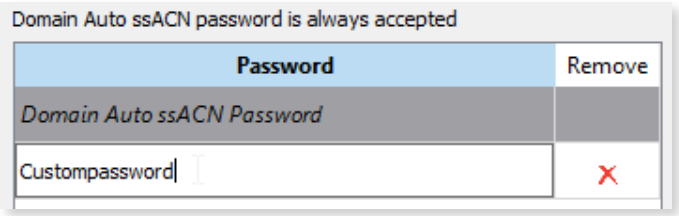
To enter a new password, click the Add Password button.



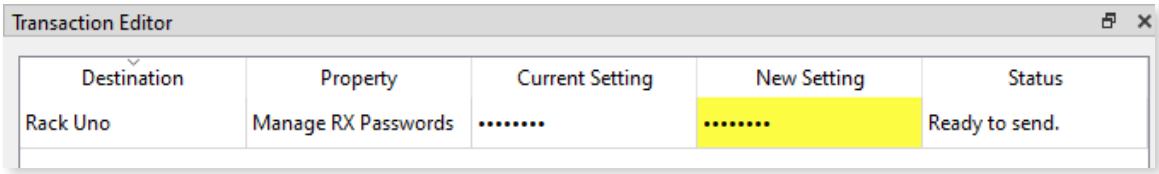
A blank entry will be added to the window.



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



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

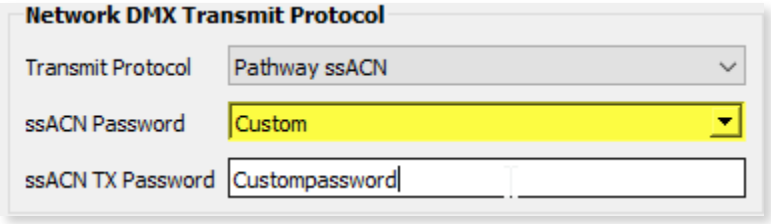


Click the Cancel button to close the window without saving any changes or edits made.

NOTE: the selected device will accept any source transmitting with a password listed in the password editor window. The Domain Auto password is always accepted.

TX (TRANSMIT) PASSWORDS

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



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

NOTES ABOUT PATHWAY ssACN

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

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

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

SOFTWARE (PATHSCAPE) CONFIGURATION

Wherever possible, we recommend using a PC with Pathscape to configure your eLink. For in-depth information on using Pathscape, see the Pathscape manual. Pathscape is available for macOS and Windows from our website: https://www.pathwayconnect.com.

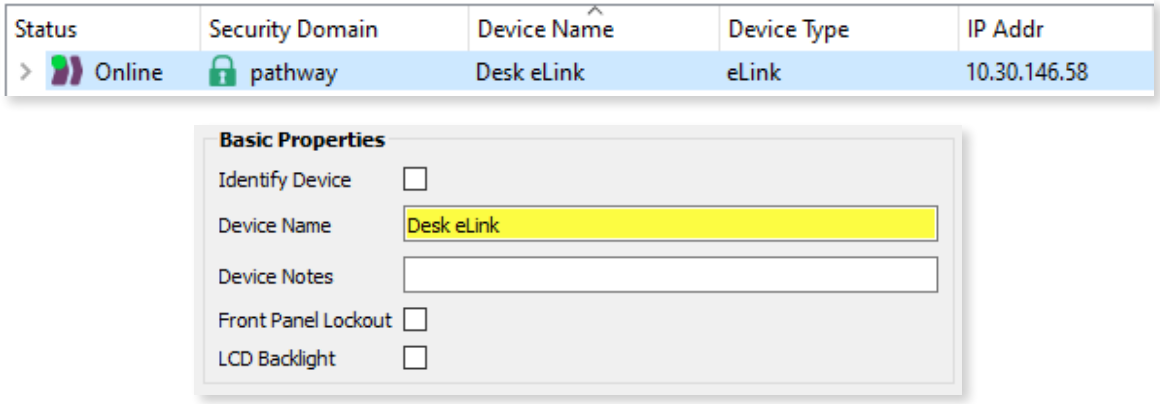
If using a PC with Pathscape is not possible or practical, see the section **Front Panel UI and Menu** later in this manual.

NETWORK SETUP

PLEASE NOTE: Before any configuration and network setup can be done, including setting the IP, the eLink 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 eLink'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 eLink's default name in the device list will be shown as its IP address. Give it a useful name before continuing.

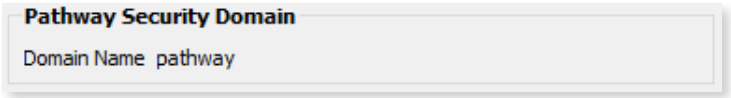


DEVICE PROPERTIES

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

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

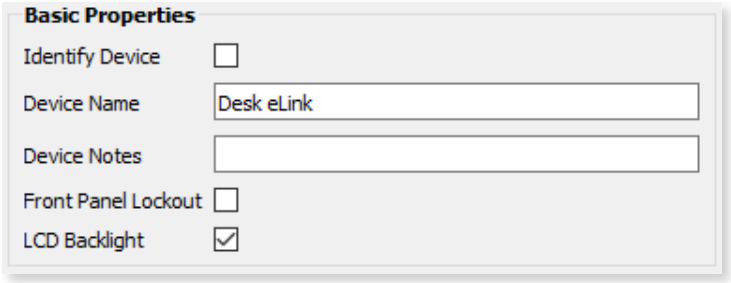
PATHWAY SECURITY DOMAIN



DOMAIN NAME

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

BASIC PROPERTIES



IDENTIFY DEVICE

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

DEVICE NAME

A user-configured, soft label for the eLink device shown in the Device window. If left blank (and by default) the device name displayed will be the device's IP Address. This label is also shown on the front LCD panel of the unit.

DEVICE NOTES

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

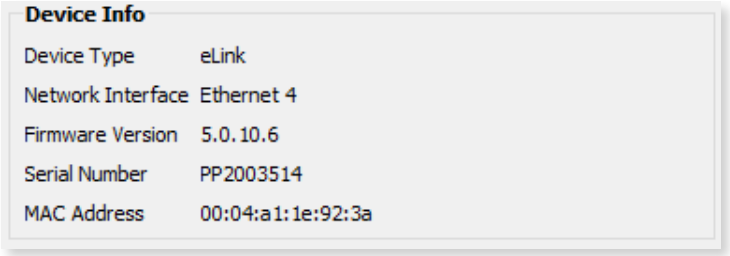
FRONT PANEL LOCKOUT

Checking this will lock the local controls on the front panel of the device. Scrolling menus allow you to read properties, but changing properties is disallowed. You can still make changes if you use the encoder within the first 30 seconds of booting the device.

LCD BACKLIGHT

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

DEVICE INFO



DEVICE TYPE

The device type for the currently selected device.

NETWORK INTERFACE

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

FIRMWARE VERSION

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

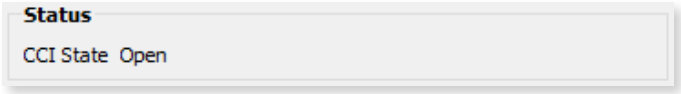
SERIAL NUMBER

Factory-set unique identifier. Read-only.

MAC ADDRESS

Factory-set hardware address. Read-only.

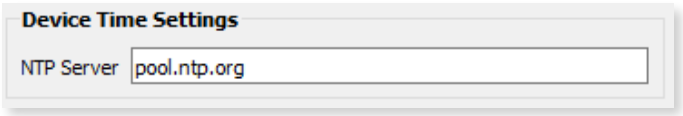
STATUS



CCI STATE

Shows the current state of the Contact Closure Interface (CCI) Input. Values are **Open** (inactive) or **Closed** (active).

DEVICE TIME SETTINGS

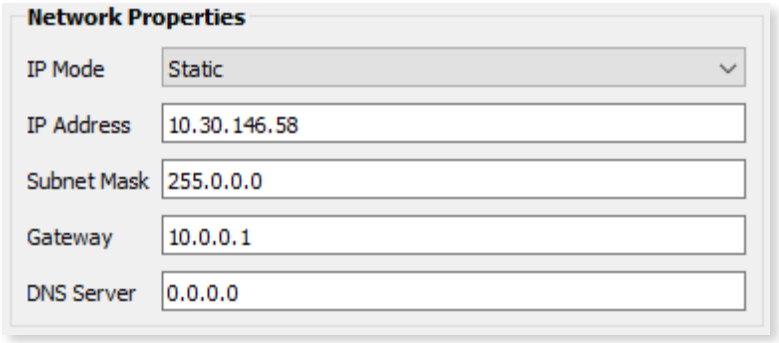


NTP SERVER

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

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

NETWORK PROPERTIES



IP ADDRESS

Internet Protocol address (IPv4) of the eLink.

SUBNET MASK

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

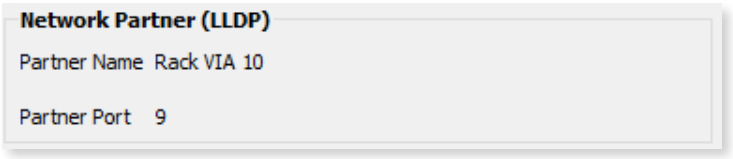
GATEWAY

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

DNS Server

Set Domain Name Server for the device here. The DNS should be specified if using and **NTP server** and/or **SixEye RMM**

NETWORK PARTNER (LLDP)



PARTNER NAME

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

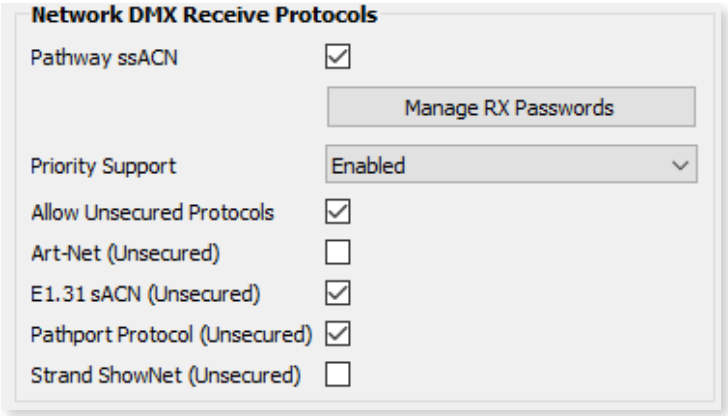
PARTNER MAC

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

PARTNER PORT

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

NETWORK DMX RECEIVE PROTOCOLS



PATHWAY ssACN

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

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

PRIORITY SUPPORT

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

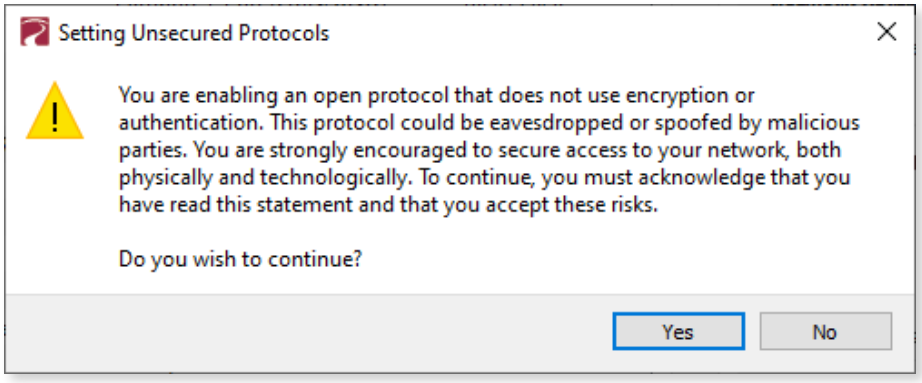
ALLOW UNSECURED PROTOCOLS

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 eLink 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 secure access to your network, both physically and technologically. To continue, you must acknowledge that you have read this statement and accept these risks.

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



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

Art-Net (UNSECURED)

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

E1.31 sACN (UNSECURED)

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

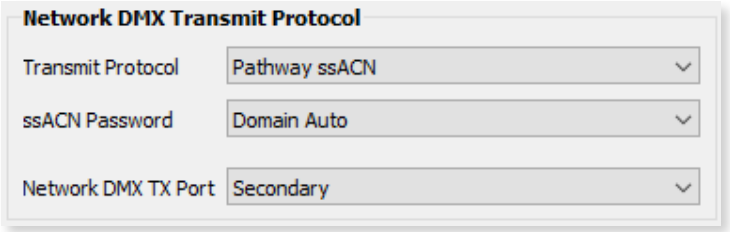
PATHPORT PROTOCOL (UNSECURED)

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

STRAND ShowNet (UNSECURED)

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

NETWORK DMX TRANSMIT PROTOCOL



TRANSMIT PROTOCOL

Use the drop-down menu to select the network protocol the eLink 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.

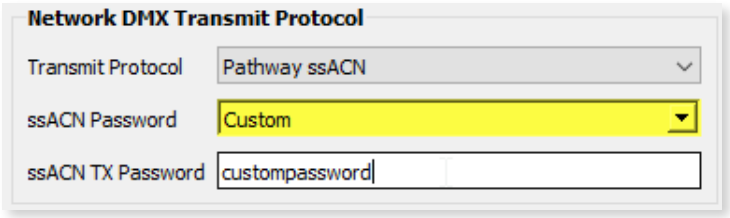
E1.31 sACN will use transmit using standard, unsecured E1.31 sACN.

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.



If **Custom** is selected, the ssACN TX Password field will appear, as shown.

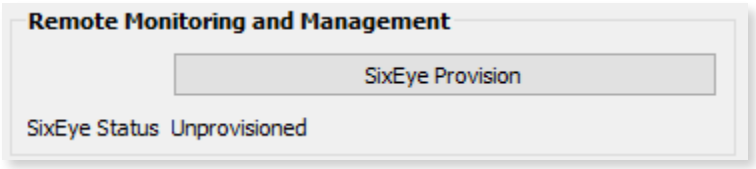
NETWORK DMX TX PORT

Specifies which **physical Ethernet port** to transmit outputs to: **Secondary** [Only], or **Primary & Secondary**.

The default value is **Secondary**. Input sources are on the Primary Port, are processed and transmitted on the **Secondary** port; the two sides are isolated from each other.

To loopback transmitted universes back onto the Primary NIC, choose **Primary & Secondary**. This is used in cases where network isolation is not required.

REMOTE MONITORING AND MANAGEMENT



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

SixEye PROVISION

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

SixEye STATUS

This shows the status of the SixEye connection.

Unprovisioned (default).

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

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

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

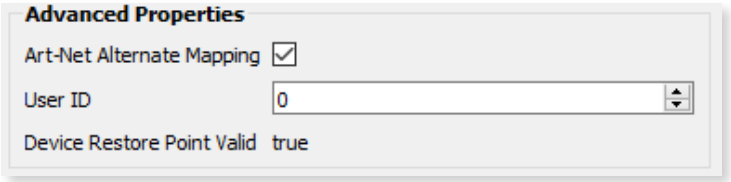
SixEye Init. The device is currently initializing a connection with SixEye.

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

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

Connected. The device is connected to SixEye.

ADVANCED PROPERTIES



ART-NET ALTERNATE MAPPING

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

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

USER ID

Custom numeric identification for external databases.

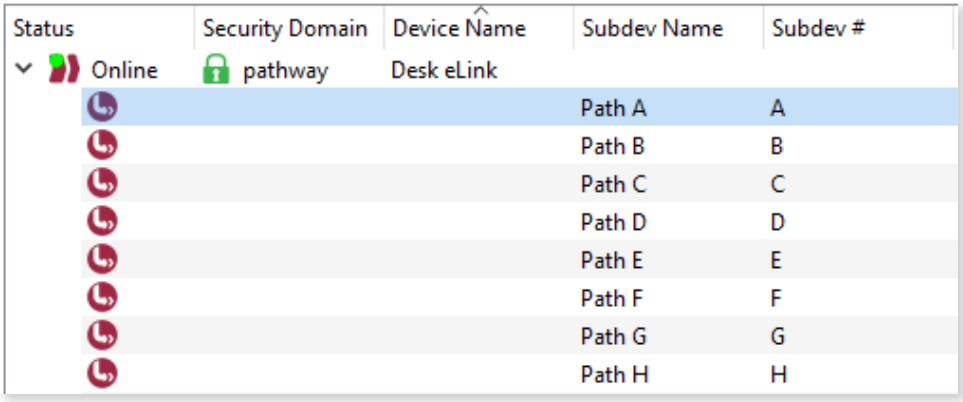
DEVICE RESTORE POINT VALID

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

PATH PROPERTIES AND CONFIGURATION

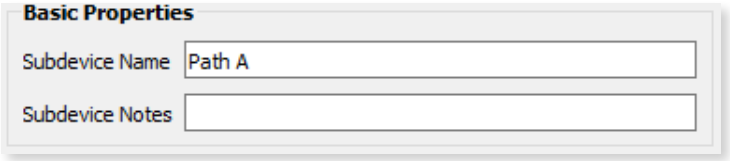
The eLink subdevices are called **Paths**. There are 16 Paths (outputs), which can each support up to 8 input sources. They support all the same Pathport-style logic you may be familiar with. They are analogous to Pathport Ports and are configured in the same manner.

Path status and properties may be reviewed by expanding the device in the device tree, and clicking on the Subdevice/Path. The properties for that Path will then be shown in the Properties Panel.



The following fields are shown in the Subdevice/Path properties panel. Some are editable, while others are read-only.

BASIC PROPERTIES



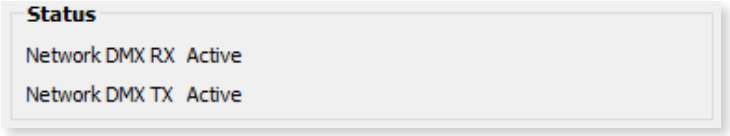
SUBDEVICE NAME

A user-configured, soft label for the Subdevice/Path. Shown in the Device view and on the front panel display of the eLink.

SUBDEVICE NOTES

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

STATUS



NETWORK DMX RX

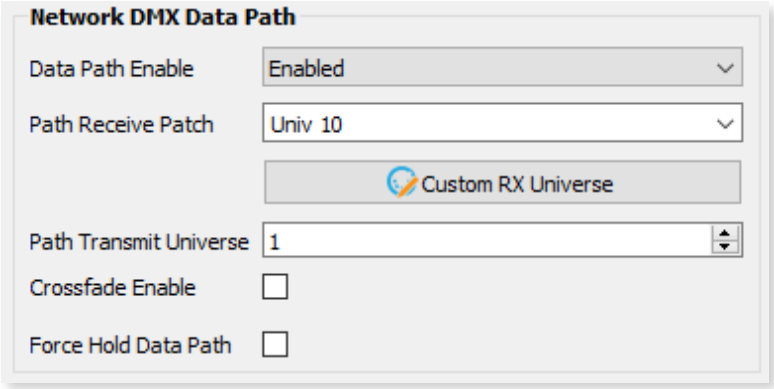
Shows status of the Network DMX source for this Path. Will show **Active** when Network DMX stream is present, and **Inactive** if Network DMX stream is lost. Read-only.

NETWORK DMX TX

Shows status of the Network DMX output of this Path. Will show **Active** when Network DMX stream is being output and **Inactive** if no Network DMX is being output. Read-only.

NOTE: In situations where source signal is lost, depending on signal loss properties (see below) it is possible for the Network DMX TX to be Active while the Network DMX RX is Inactive.

NETWORK DMX DATA PATH



DATA PATH ENABLE

For debugging purposes or otherwise, you may want to disable an eLink Network Path. All other properties remain unchanged.

Use the drop-down menu to choose **Enabled** (default) or **Disabled**.

PATH RECEIVE PATCH

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

CUSTOM RX UNIVERSE

To create a custom patch for the receive Path, click the **Custom RX Universe** button to open the **Custom Universe Editor**.

See the section later in this manual under **Custom Receive Patch** for detailed instructions.

PATH TRANSMIT UNIVERSE

Enter the Universe number you wish to transmit this Path output to.

CROSSFADE ENABLE

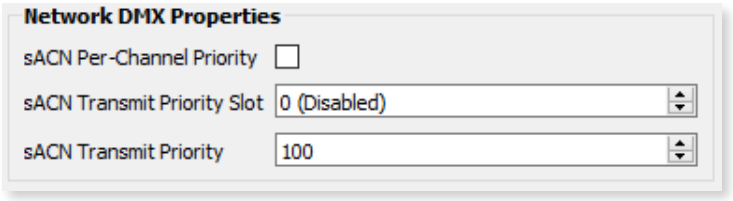
If a Priority changes either as defined by the Custom RX Universe patch priorities or the E1.31 sACN/Pathway ssACN Priority, the output will fade rather than snap to the new levels. The last frame of the old source is frozen during the fade.

FORCE HOLD DATA PATH

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

This property can be set by Pathscape, or configured to be controlled by the Contact Closure on the rear of the eLink (see **CCI Action** below), or through the SixEye cloud.

NETWORK DMX PROPERTIES



sACN PER-CHANNEL PRIORITY

In the base eLink device's **Network DMX Receive Protocols**, there is a property **Priority Support** which determines if the device 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.

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 Path 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 FOREVER

If enabled, Signal Loss **Hold Time**, Signal Loss **Fade to Black** and Signal Loss **Port Shutdown** are not shown. The Path Output will continue outputting the last received packet indefinitely in the event of Network DMX Receive signal loss.

HOLD TIME (s)

The Path will continue transmitting its last packet it received until this time has expired.

FADE TO BLACK

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

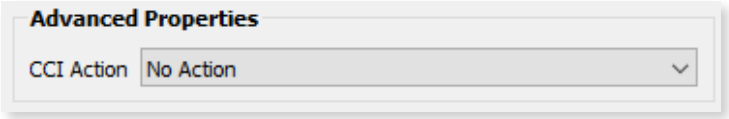
FADE TIME (s)

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 Receive stream ceases and the Fade Time has expired, the Path Output will turn off. This is **enabled** by default.

ADVANCED PROPERTIES



CCI ACTION

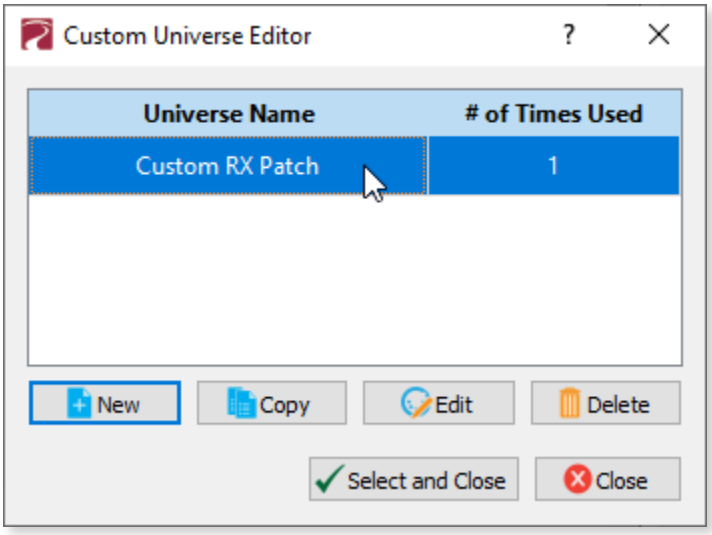
Choose the function of the CCI input, if desired. When the Contact Closure Interface is **closed** (activated), the chosen action will be performed on the selected port.

No Action: No action is taken.

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

CUSTOM RECEIVE PATCH

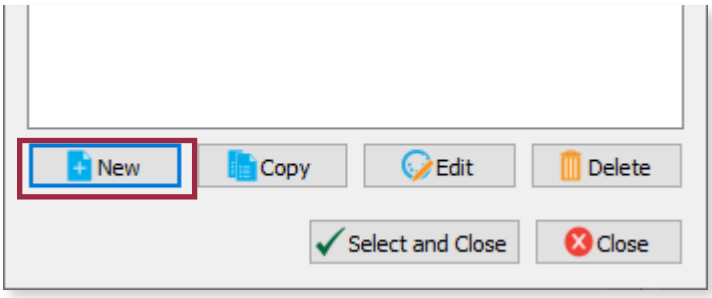
To create a custom patch for the receive Path, click the **Custom RX Universe** button under the **Network DMX Data Path** section of the Subdevice (Path) properties. This will open the **Custom Universe Editor**.



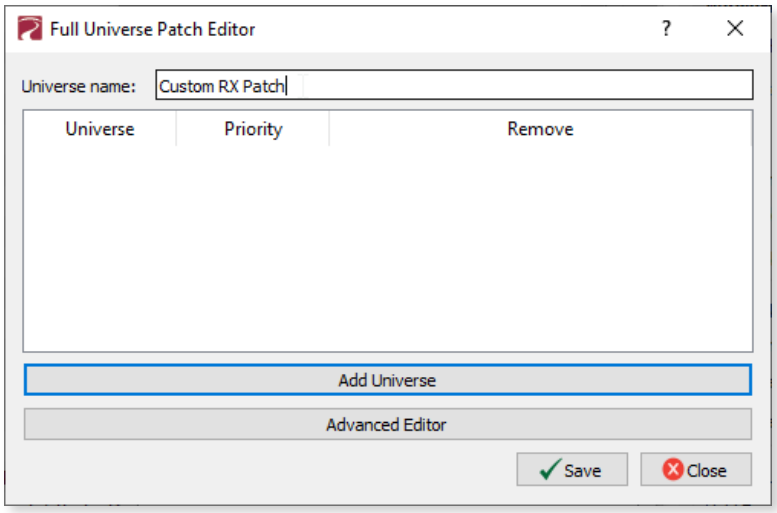
The **Custom Universe Editor** window is used to configure the custom receive patches for each Path, by adding the Pathport-like logic like merging input universes at configurable priority levels.

You may **Add New Custom Universes**, and **Copy**, **Edit** or **Delete** existing ones. Pathscape also will show **how many times** each Custom Patch is being used by any Pathport Port or eLink Path on your network.

To create a custom patch, click the New button at the bottom of the **Custom Universe Editor** window.



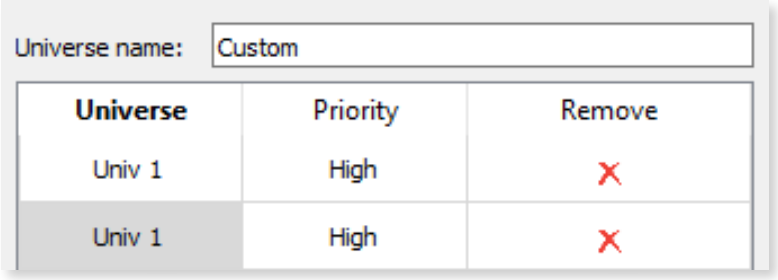
This will bring up the **Full Universe Patch Editor** window.



At the top of the window, enter a name for the custom patch under **Universe Name:**. By default, the field is filled with the text “Custom”.

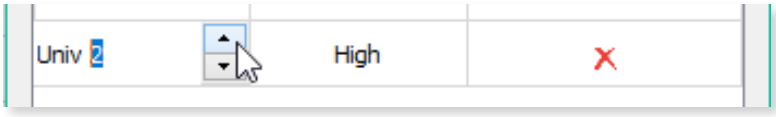
There are two buttons at the bottom of the window: **Add Universe** and **Advanced Editor**.

For simple custom patches, such as merging multiple universes, click the Add Universe button. This will add one Universe row with the following columns: **Universe**, **Priority** and **Remove**.

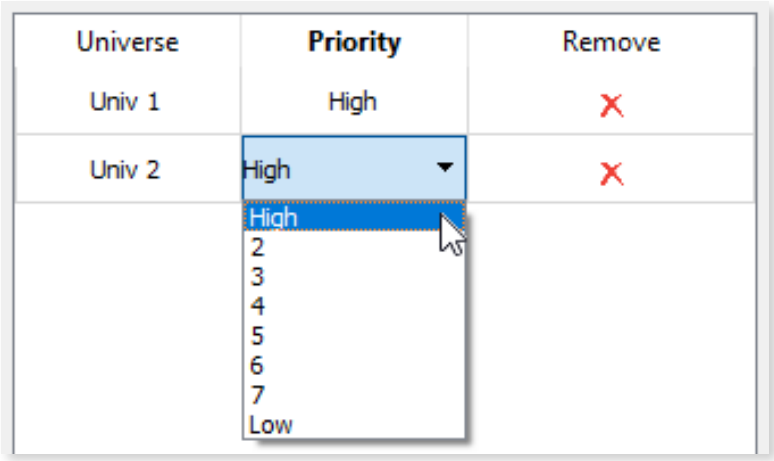


The **Universe** column shows the source Universe, the **Priority** column the Priority (default is High) and the **Remove** column allows you to click the X to delete an unwanted entry.

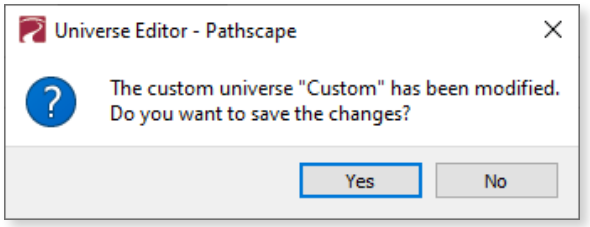
To select the desired Universe, double-click on the “**Univ 1**” cell. You can then use the up and down arrows to select the desired Universe. You may also directly type in the Universe number.



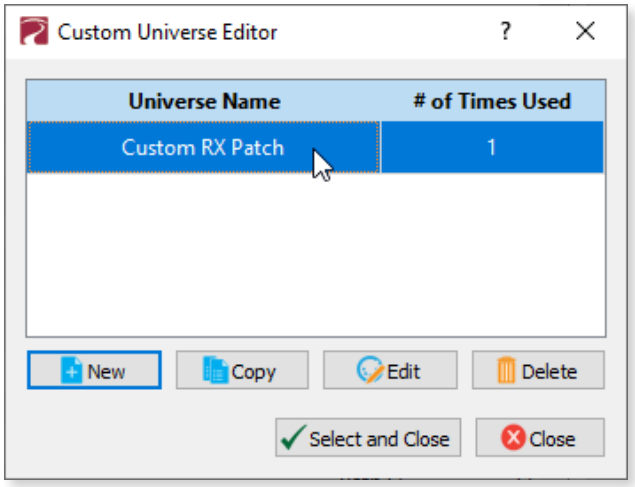
To select the Priority level of the source, double-click the **Priority** cell, marked with “High” by default. You may then choose a priority level in the drop-down menu.



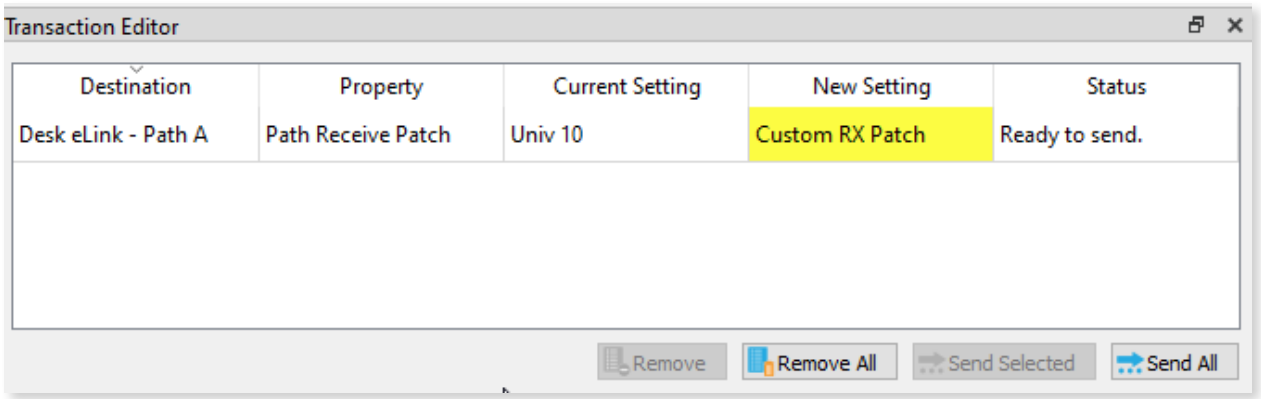
Once you are satisfied, click the Save button. To discard changes, click the Exit button. You will then have another chance to save changes, or discard them.

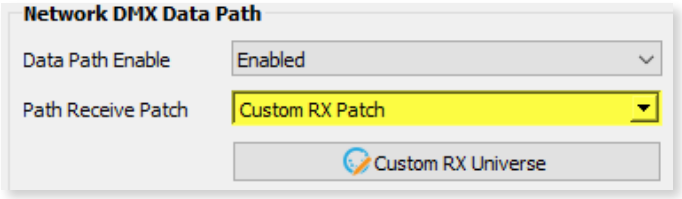


Your new custom patch will be shown in the Custom Universe Editor window. Select the Custom Patch name and click the Select and Close to set the path to that patch. Click the Close button to discard changes.



A transaction will then be queued in the Transaction Editor, which must be sent in order to commit changes.



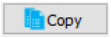


COPYING, EDITING AND DELETING CUSTOM PATCHES

Once you have created a custom patch, you may wish to make changes to it, make a copy and then make changes to that copy, or simply delete unneeded patches.

To **edit** an existing custom patch, open the **Custom Universe Editor** and click on the custom patch name, then click the 

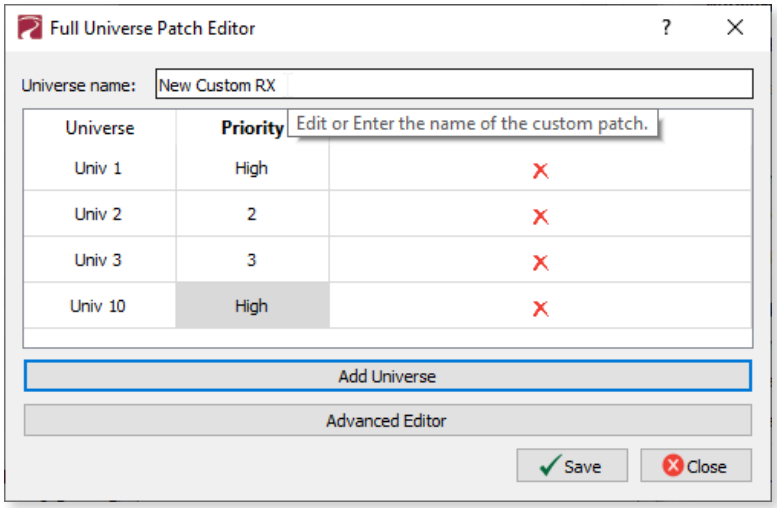
button.

To **copy** a custom patch, click the patch name, then click the 

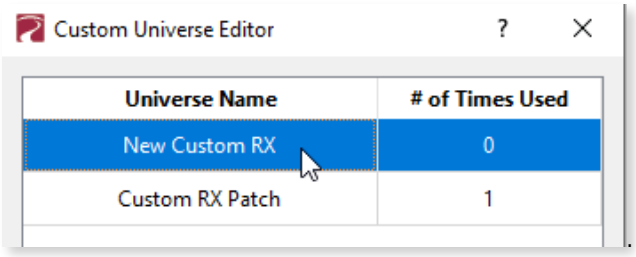
button. This will open the Full Universe Patch Editor window, showing a copy of the custom patch with all its settings.

Make any edits here to the new copy of the patch, and click 

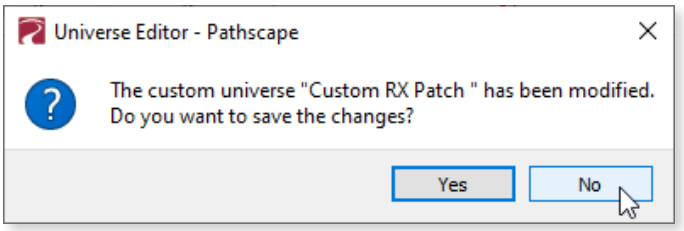
to save the copy as a new custom patch.



The new custom patch will then be listed in the Custom Universe Editor, where you may select it for patching to the RX path.

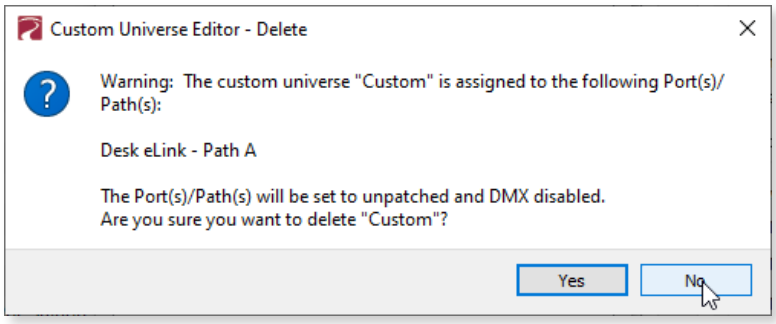


To discard changes to the copy of the patch, click the Close button. A confirmation dialog will appear, allowing you to save those changes instead, or continue with discarding the changes.



If the changes are discarded, no copy of the patch will appear in the Custom Universe Editor window.

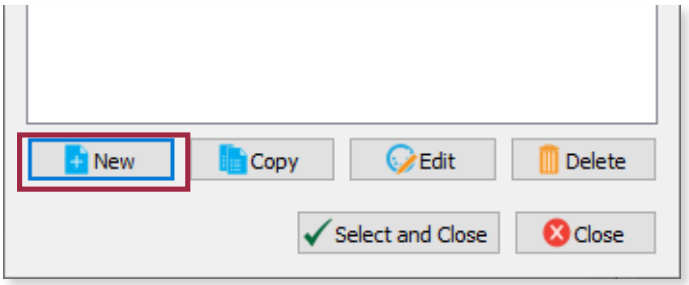
To **delete** a patch, click anywhere in the patch column and click the Delete button. If the selected patch is currently assigned to a path, a warning dialog will appear, asking for confirmation of deletion.

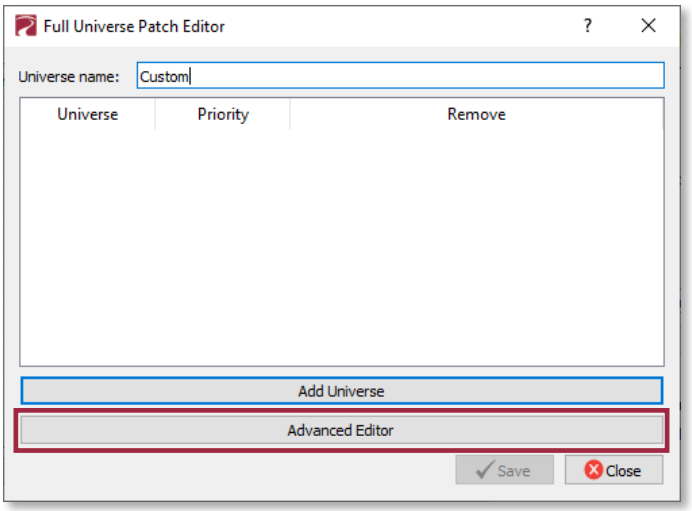


If the selected patch is not currently assigned to a Path, there is **no confirmation dialog** when clicking the Delete Patch button; it will be immediately deleted.

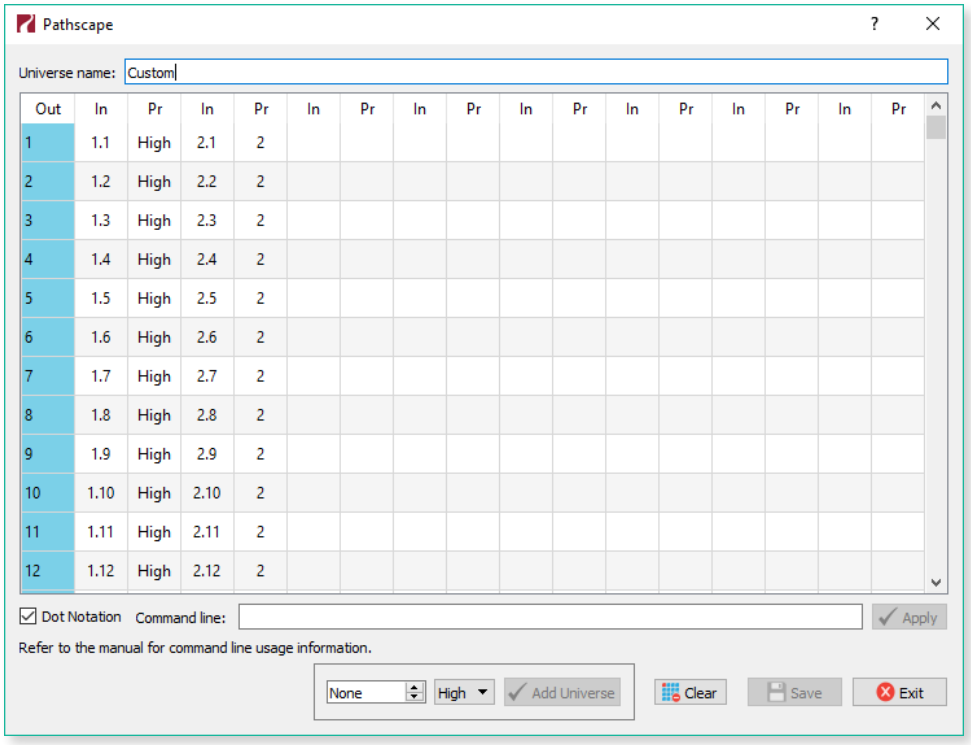
ADVANCED PATCH EDITOR

For more advanced custom receive patch editing, use the **Advanced Editor**. Click on the New button at the bottom of the Custom Universe Editor window, then click the **Advanced Editor** button at the bottom of the Patch Editor window.





The **Advanced Editor** window will open.



The Advanced Editor will allow you to set priority on a channel-by-channel basis, as well as configure specific ranges of channels, e.g. non-contiguous ranges or small ranges of channels.

The Advanced Editor window has several columns: **Out**, and then **In** and **Pr**, repeating for a total of 8 possible inputs.

The **Out** column refers to the output of the patch, and has 512 rows, one for each channel.

The **In** column and **Pr** column work together. The **In** column is for specifying the input universe and channel, and the **Pr** column for setting the priority level of that channel, which is then patched to the output channel of the same row.

There are several ways to enter channel values.

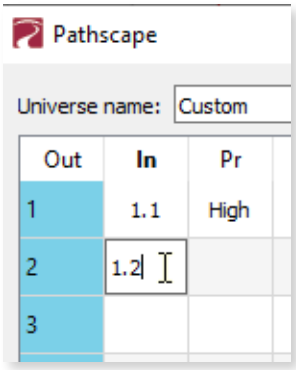
INPUTTING CHANNELS AND PRIORITIES

ENTERING VALUES MANUALLY

If you have only a handful of channels to configure, you can enter them manually typing them directly into the table cells. By default, the syntax is: "**Universe.Slot**", i.e. "1.1" is Universe 1, Slot 1 and "1.512" is Universe 1, Slot 512.

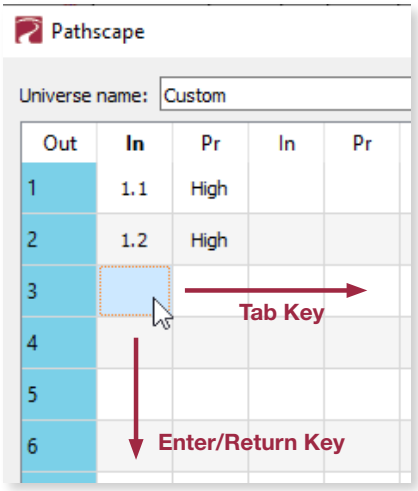
NOTE if you type a single number, it will convert it to the correct universe. For example, if you just type "3" it will change to "1.3". If you type "513", it will convert to "2.1".

Double-click on a cell, and type in the channel number.



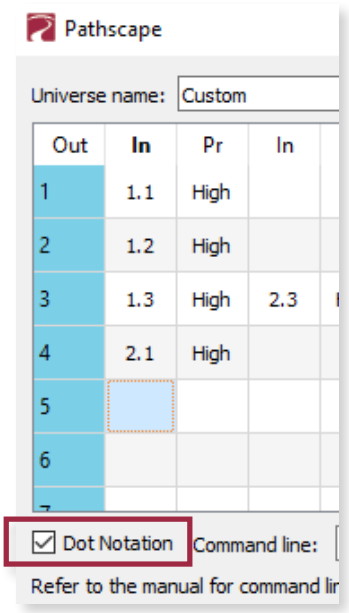
In this example we typed in channels 1 (first row) and 2 (second row) from Universe 1

You can also click on a cell to highlight it, and begin typing directly. Press the **Tab** key to accept your entry and move two cells to the **right** (one In/Pr pair to the right); press the **Enter/Return** key to accept your entry and move one cell **downwards**. Note that the default priority when typing any value into a cell is **High**.



Hitting the **Tab** key **without typing** any values into a cell will move the selected cell **one** space to the right. Hitting **Tab** at the end of a row will select the first cell of the next row downwards. Note that hitting the Enter/Return key without typing a value into a cell will do nothing.

To change the way Pathscape displays the channels, the ☑ Dot Notation checkbox is provided in the bottom-left corner of the window.

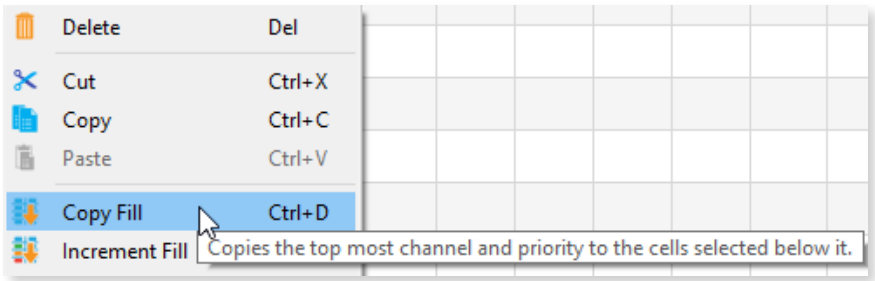


By default, it is checked; which displays the channels in the "X.Y" format. Uncheck this box if you prefer to see the absolute channel number (1-512 for Universe 1, 513-1024 for Universe 2, and so on).

For example, to enter Universe 1 channel 1 into the first cell, click on the cell and type in "1.1". You may also type in the absolute channel number. Pathscape will do the conversion for you, depending on the status of the ☑ Dot Notation item.

USING THE COPY FILL FUNCTION

There are two "Fill Channel" functions under the right-click menu, **Copy Fill** and **Increment Fill**.



These are both useful to filling in several channels without having to manually enter them.

Both of these require at least one pre-existing value. For example, enter "1.1" in the first cell.

To extend the same channel patch to a range of output channels, select the first cell and shift-click to select a range of cells downward. In this example, rows 1 through 10 are selected.

With the selection made, right-click and select **Copy Fill**. This will copy the values from the first cell and apply them to all selected cells. If you need the same input channel to be patched to several output channels, this is a much faster method than manually entering them.

Out	In	Pr
1	1.1	High
2		
3		
4		
5		
6		
7		
8		
9		
10		

Out	In	Pr
1	1.1	High
2	1.1	High
3	1.1	High
4	1.1	High
5	1.1	High
6	1.1	High
7	1.1	High
8	1.1	High
9	1.1	High
10	1.1	High

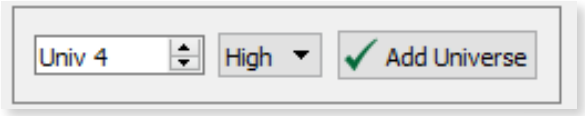
The **Increment Fill** is similar, but will increment each channel by 1. Using the same start value as the above example, but choosing **Increment Fill**, we get the following result.

Out	In	Pr
1	1.1	High
2	1.2	High
3	1.3	High
4	1.4	High
5	1.5	High
6	1.6	High
7	1.7	High
8	1.8	High
9	1.9	High
10	1.10	High

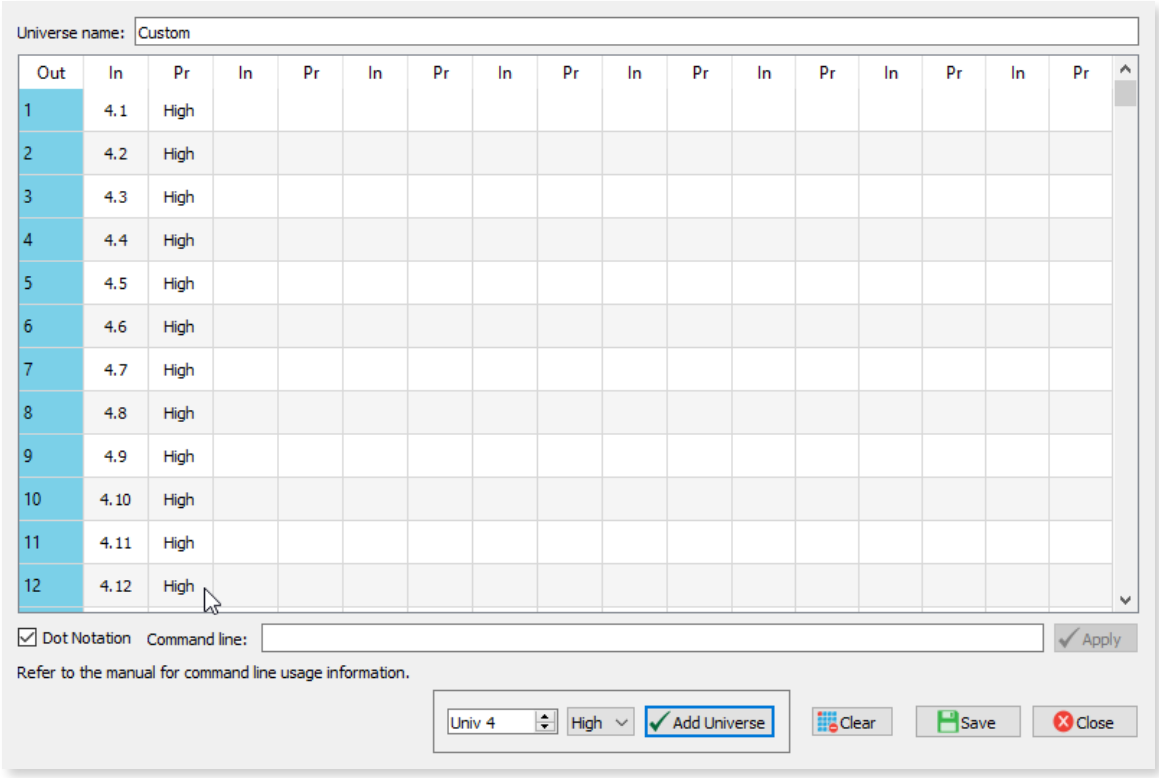
This is useful for filling in contiguous ranges of channels quickly without manually entering them.

USING THE ADD UNIVERSE FUNCTION

Another way to input channel ranges is using the **Add Universe** box at the bottom of the window.



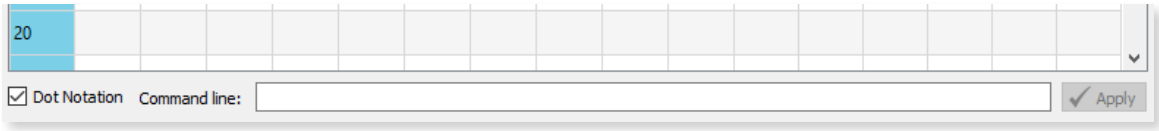
This works essentially the same as the basic Full Universe Patch Editor window. Select a Universe using the up and down arrows, or type it directly into the text field, select the priority level, and click the **Add Universe** button. This will fill the first available **In** and **Pr** columns with the selected channel and priority information.



At this point you may want to edit specific channels or channel ranges within that universe, which you can do manually or using the **Fill Channel** items.

USING THE COMMAND LINE

At the bottom of the window, above the **Add Universe** section, is the **command line**. This can be used to create entire patches in a single command.



The syntax for the command line is as follows:

Output Range AT Input Range [(At Equal Priority/At Next Lowest Priority)Additional Range]

This might look a little confusing but let's break it down.

Item/Character	Description
- (dash)	Used for ranges (optionally a range can have a starting value, then a dash and no ending value, if using the entire 1-512 slot range)
* (asterisk)	Used for AT
+ (plus sign)	Used to add next range at equal priority
/ (slash)	Used to delineate next lowest priority (note you cannot use the command line to specify a priority specifically)
, (comma)	Simple value separator
. (period)	Used to specify **Universe.Slot** notation
[ ] (square brackets)	Optional Entries

Output Range is the range of output channels to which we are assigning input channels. Let's use the full universe in this example (slots 1-512).

Input Range is the range of input slots we'd like to patch to those outputs (in the "**Universe.Slot**" format mentioned earlier). Let's use Universe 1 for this example, so our range would be **1.1-1.512**.

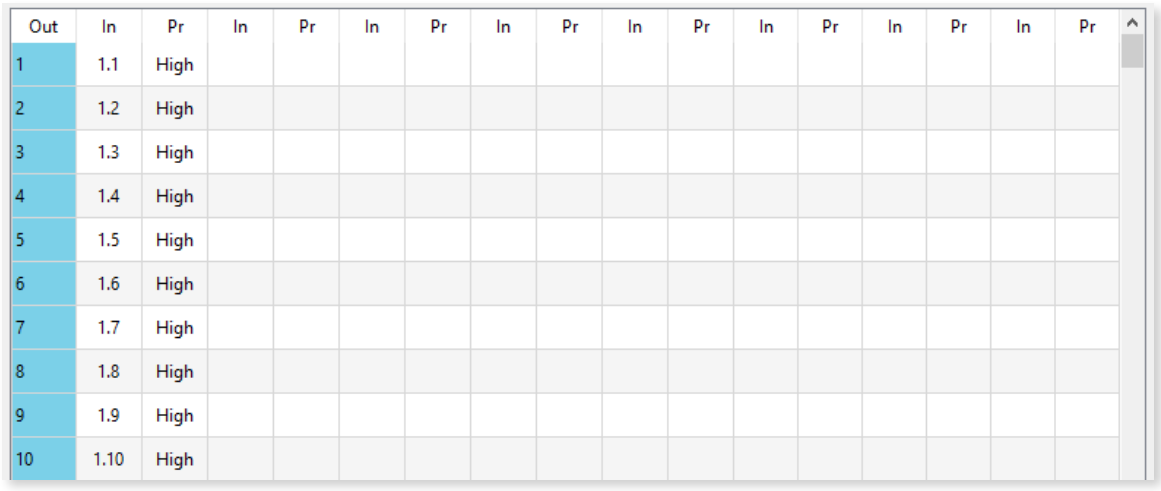
AT is an operator character, the "*****" (asterisk).

The elements inside the **square brackets** are optional, so let's forget them for now. Our command looks like this:

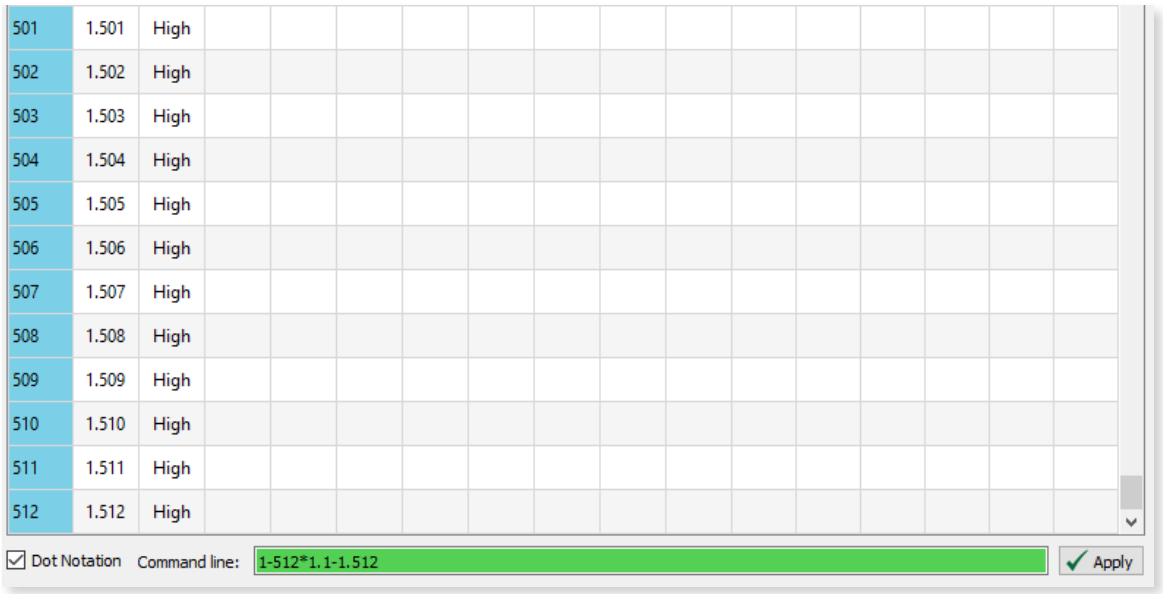
1-512*1.1-1.512

Hit the enter key or click the 

button to send the command. We should have something like this:



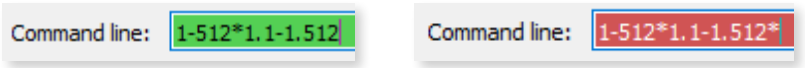
Out	In	Pr	In	Pr	In	Pr	In	Pr	In	Pr	In	Pr	In	Pr	In	Pr
1	1.1	High														
2	1.2	High														
3	1.3	High														
4	1.4	High														
5	1.5	High														
6	1.6	High														
7	1.7	High														
8	1.8	High														
9	1.9	High														
10	1.10	High														



(Middle of the window not shown)

The command should have entered 1.1 through 1.512 as the Input channels in the **In** column, and filled in the **Pr** column with the value **High**.

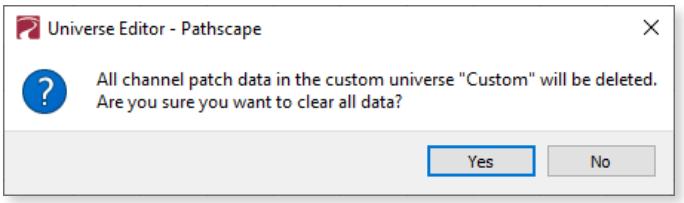
NOTE: the Command Line field will highlight in **green** if the command syntax is valid, and **red** if it is not valid.



Valid syntax (left), Invalid syntax (right)

To clear the entire patch window, click the 

button in the bottom-right corner. A confirmation dialog will appear.



Confirm by clicking **Yes**, so we can try another command.

To add additional ranges using the same command, use the "**+**" (plus sign) or the "**/**" (forward slash) characters.

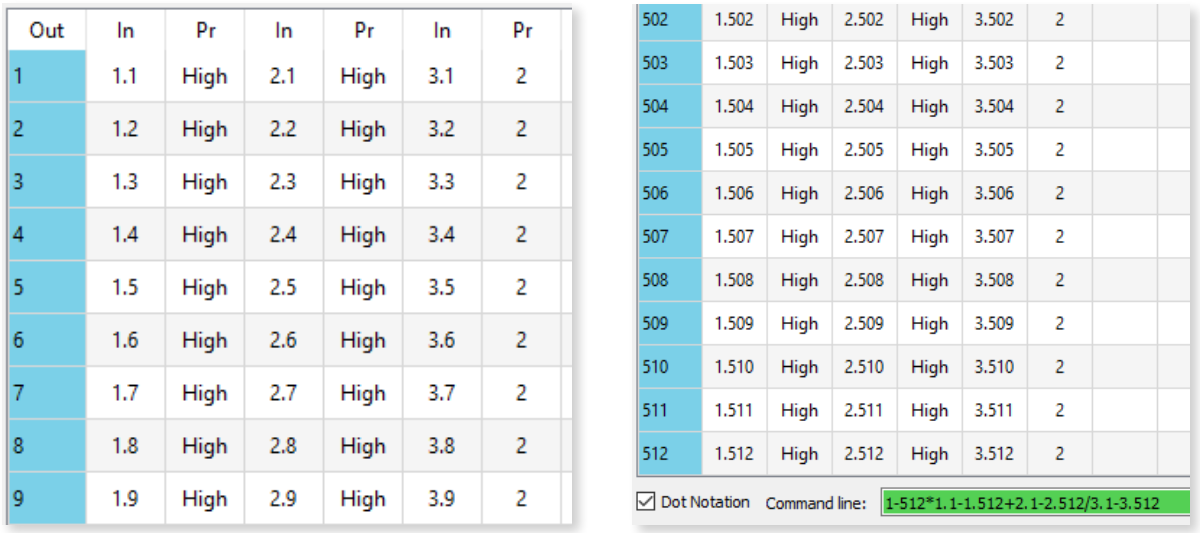
The "**+**" character adds the next range of channels **at equal priority** as previous, while the "**/**" character adds the next range **at next lowest priority**.

Let's try another command and add 2 ranges to the initial example; Universe 2 at the same priority (using the "+" character) and Universe 3 at the next lowest priority (using the "/" character).

Our command would now look like this:

1-512*1.1-1.512+2.1-2.512/3.1-3.512

And our Patch Window should look like:



Out	In	Pr	In	Pr	In	Pr
1	1.1	High	2.1	High	3.1	2
2	1.2	High	2.2	High	3.2	2
3	1.3	High	2.3	High	3.3	2
4	1.4	High	2.4	High	3.4	2
5	1.5	High	2.5	High	3.5	2
6	1.6	High	2.6	High	3.6	2
7	1.7	High	2.7	High	3.7	2
8	1.8	High	2.8	High	3.8	2
9	1.9	High	2.9	High	3.9	2
502	1.502	High	2.502	High	3.502	2
503	1.503	High	2.503	High	3.503	2
504	1.504	High	2.504	High	3.504	2
505	1.505	High	2.505	High	3.505	2
506	1.506	High	2.506	High	3.506	2
507	1.507	High	2.507	High	3.507	2
508	1.508	High	2.508	High	3.508	2
509	1.509	High	2.509	High	3.509	2
510	1.510	High	2.510	High	3.510	2
511	1.511	High	2.511	High	3.511	2
512	1.512	High	2.512	High	3.512	2

With the one command, we added:

- Universe 1, channels 1 through 512 at High priority (the original "**1-512*1.1-1.512**" command)
- Universe 2, channels 1 through 512 at the same (High) priority (the "**+2.1-2.512**" part), and
- Universe 3, channels 1 through 512 at the next lowest priority (2) (the "**/3.1-3.512**" part).

In the command syntax, "range" can be any range of channels; it does not have to be the full universe of 1-512. We could change the ranges in the above example from 1-512 to 1-10 (and also change **1.1-1.512** to **1.1-1.10**, and so on for Universe 2 and 3) and we would patch only channels 1 through 10.

The command would then look like:

1-10*1.1-1.10+2.1-2.10/3.1-3.10

Out	In	Pr	In	Pr	In	Pr	In
1	1.1	High	2.1	High	3.1	2	
2	1.2	High	2.2	High	3.2	2	
3	1.3	High	2.3	High	3.3	2	
4	1.4	High	2.4	High	3.4	2	
5	1.5	High	2.5	High	3.5	2	
6	1.6	High	2.6	High	3.6	2	
7	1.7	High	2.7	High	3.7	2	
8	1.8	High	2.8	High	3.8	2	
9	1.9	High	2.9	High	3.9	2	
10	1.10	High	2.10	High	3.10	2	
11							
12							

The example from above with channels 1-512 changed to 1-10.

NOTE: if the full range of channels is going to be used (1-512), the second number is technically **not required**. For example, to specify the output range of **1-512**, we can simply drop the "512" and type "**1-**". Pathscape assumes we mean the full range of 1-512. We can do the same with the input range. Instead of typing "**1.1-1.512**" we can simply type "**1.1-**".

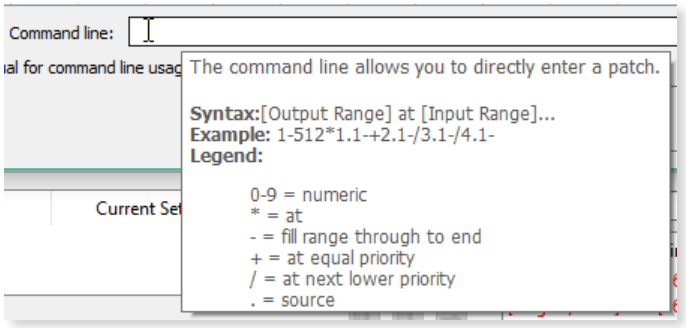
The command from the example on the previous page could then be written:

1-*1.1-+2.1-/3.1-

Which is much faster to type, but maybe a little harder to understand at a glance. Use whatever method you prefer.

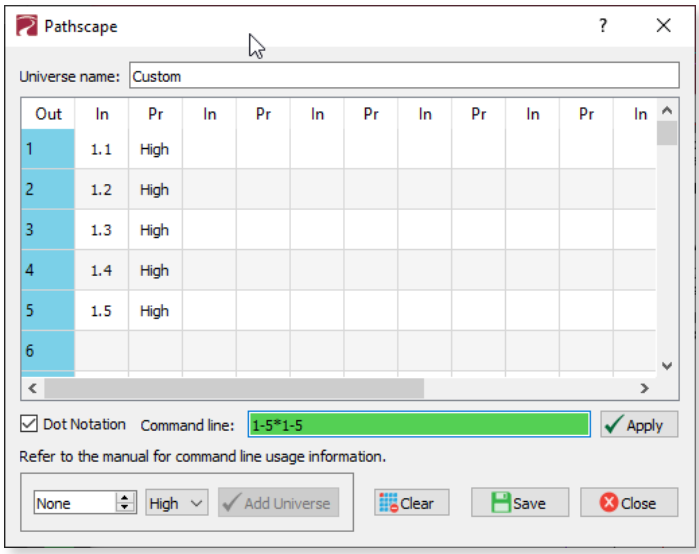
Keep in mind that if we want to use the command line to patch a range of channels **less** than the full 1-512 range, the second number is **required**.

Note: if you hover the cursor over the Command Line field, a tool tip will pop up with a reminder of the syntax and an example command.

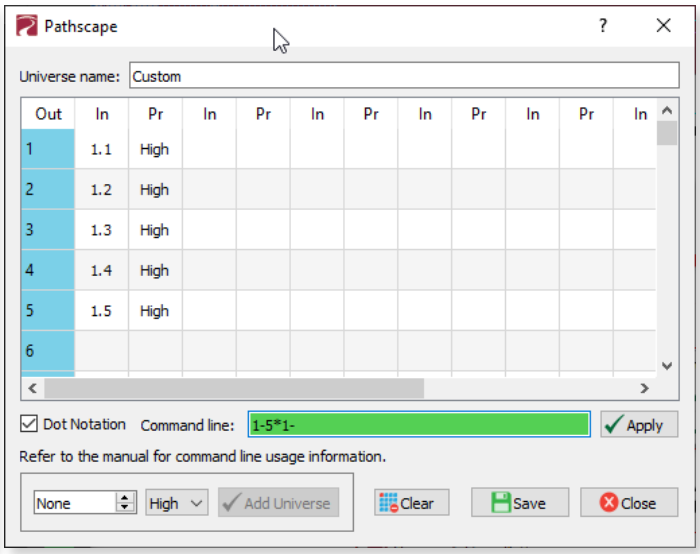


ADVANCED PATCH EDITOR EXAMPLES

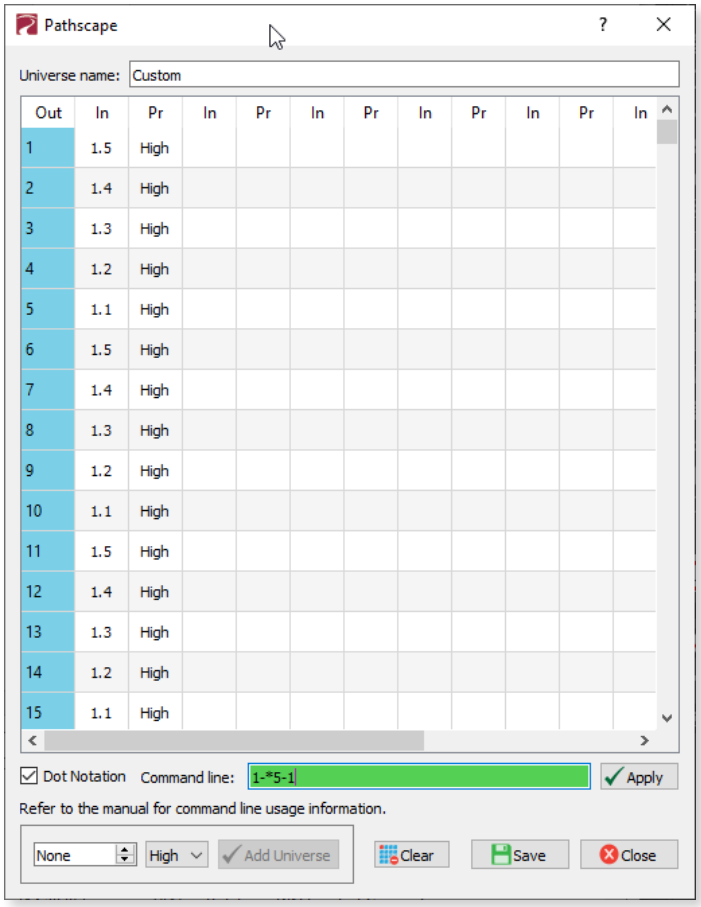
See below for some more examples of using the Advanced Patch Editor.



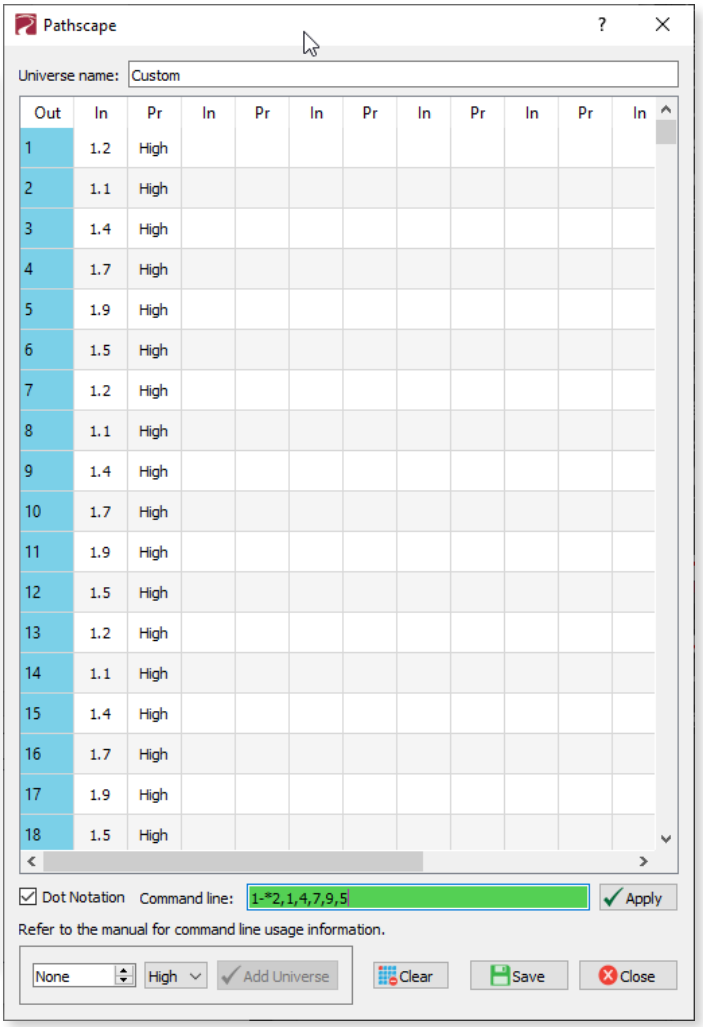
Command line: 1-5*1-5



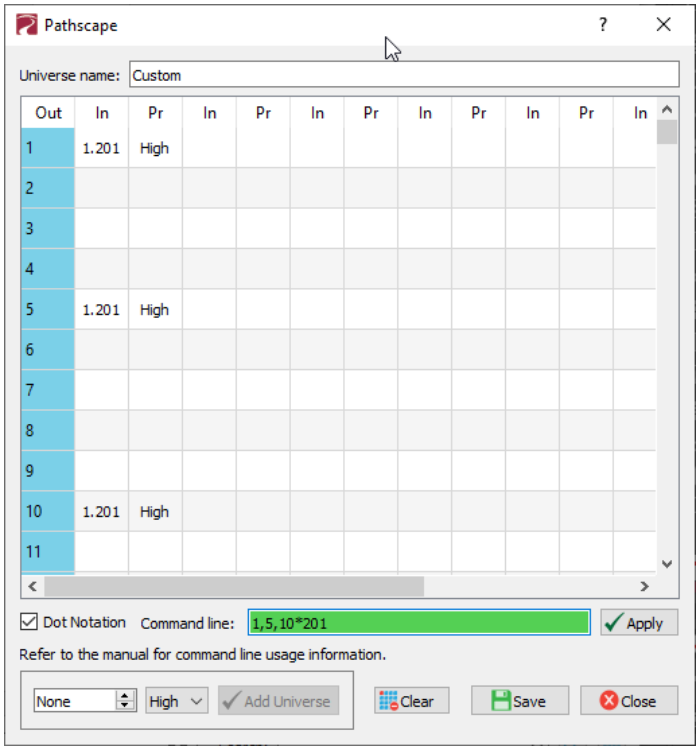
Command line: 1-5*1-



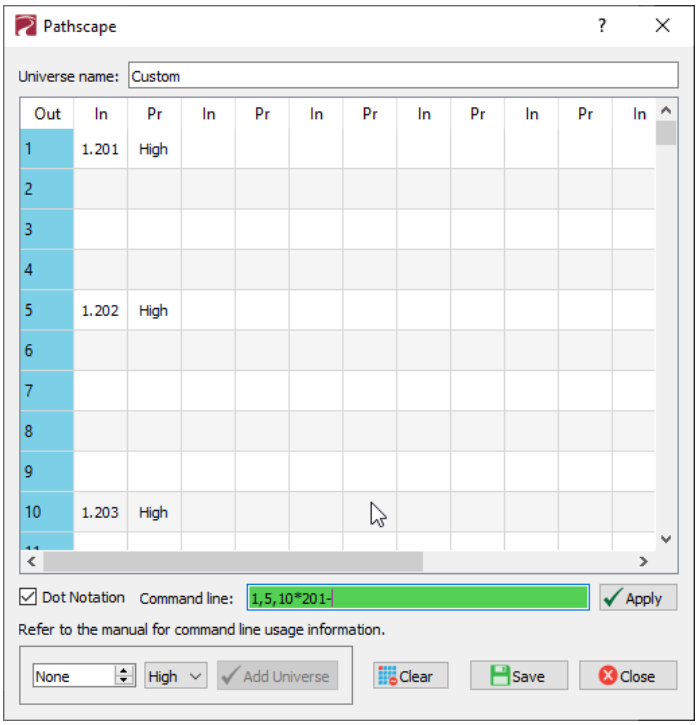
Command line: 1-*5-1



Command line: 1-*2,1,4,7,9,5



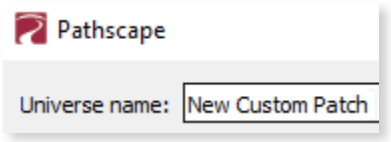
Command line: 1,5,10*201



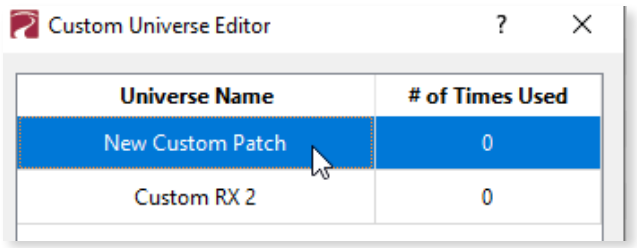
Command line: 1,5,10*201-

SAVING OR DISCARDING CUSTOM PATCH

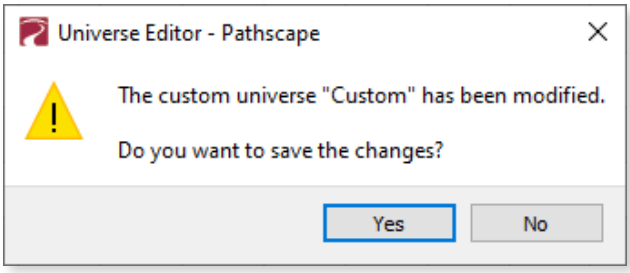
To save the custom patch, click the Save button in the bottom-right corner of the window. Make sure to give your custom patch a name at the top of the window.



Once saved, the Save button will become grayed out, and you may exit the window by clicking the Close button. Your new custom patch will be added to the **Custom Universe Editor** window.



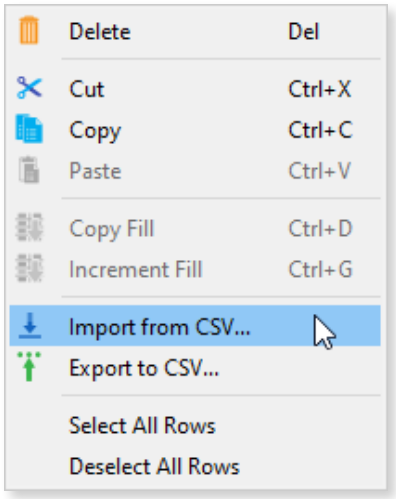
To discard the changes made and exit the Advanced Patch window without saving, click the Close button. A confirmation dialog will appear, giving you a last chance to save changes to the custom patch.



Click "**No**" to discard changes and return to the main Pathscape window. Clicking "**Yes**" will save the custom patch with its current name and settings.

USEFUL RIGHT-CLICK MENU ITEMS

In the Advanced Patch Editor, there are several helpful functions in the right-click menu. Right-click in the main channel grid area to see the menu.



Delete will delete any selected cells. You may also use the **DEL/Backspace** key. You can delete multiple cells by shift- or control-clicking to select multiple ranges, both contiguous and non-contiguous.

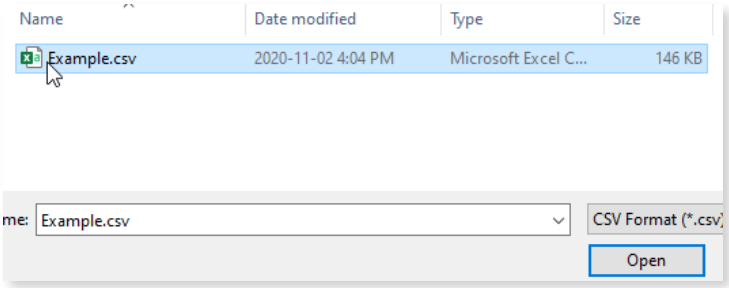
Cut will cut any selected cells for pasting elsewhere in the channel patch grid.

Copy will copy any selected cells for pasting elsewhere in the channel patch grid.

Paste will paste any copied/cut cell values, starting on the selected cell.

Copy Fill and **Increment Fill** are explained in the **Using the Copy Fill Function** section above.

Import from CSV... will import values from a Comma Separated Value (CSV) file generated from Pathscape and input them into the channel patch grid. Click this item and a **Open File Dialog** will appear. Choose a CSV file, and click the "**Open**" button.



	A	B	C	D	E	F	G	H	I	J
3	!patch	outChannel	inChannel1	inPri1	inChannel2	inPri2	inChannel3	inPri3	inChannel4	inPri4
4	patch	1	1	1	513	8	1025	4		
5	patch	2	2	1	514	8	1026	4		
6	patch	3	3	1	515	8	1027	4		
7	patch	4	4	1	516	8	1028	4		
8	patch	5	5	1	517	8	1029	4		
9	patch	6	6	1	518	8				

CSV File Contents

Universe name: Example

Out	In	Pr	In	Pr	In	Pr	In	P
1	1.1	High	2.1	Low	3.1	4		
2	1.2	High	2.2	Low	3.2	4		
3	1.3	High	2.3	Low	3.3	4		
4	1.4	High	2.4	Low	3.4	4		
5	1.5	High	2.5	Low	3.5	4		
6	1.6	High	2.6	Low				
7	1.7	High	2.7	Low				
8	1.8	High	2.8	Low				
9	1.9	High	2.9	Low				
10	1.10	High	2.10	Low				
11	1.11	High	2.11	Low				
12	1.12	High	2.12	Low				

Advanced Editor fills in values from CSV File

Export to CSV... will export the current channel patch grid to a CSV file for importing onto a different machine. Click this item and a **Save File Dialog** will appear, enter a name for the file and click "**Save**".

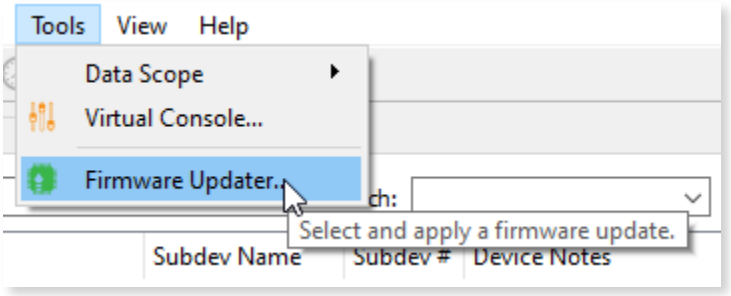
Select All Rows will select all rows and **Deselect All Rows** will deselect them.

UPGRADING DEVICE FIRMWARE

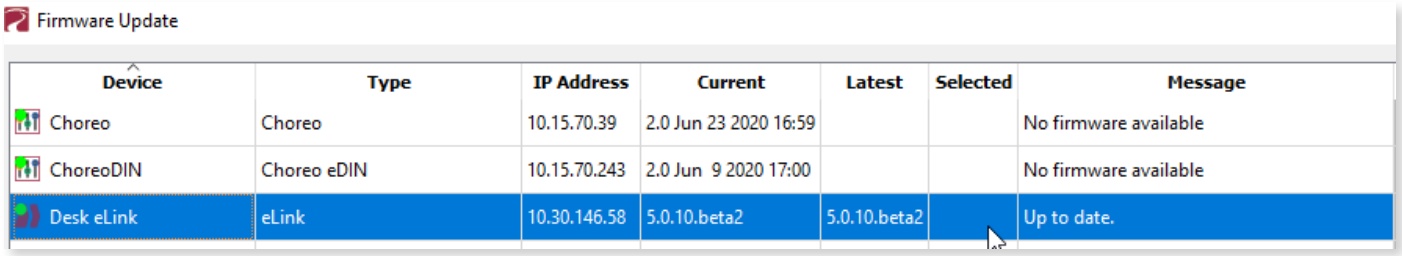
Firmware upgrades may only be done using Pathscape.

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

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



This will bring up the Firmware Update window.



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

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

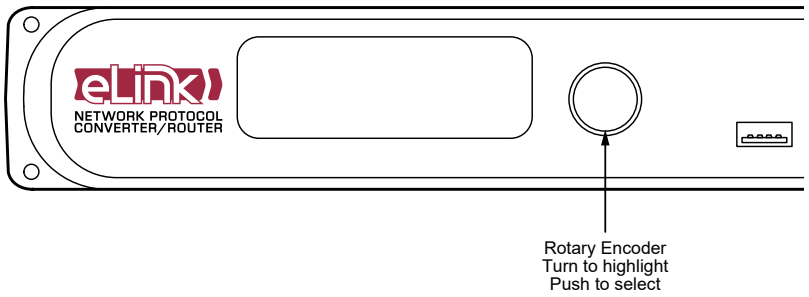
It is strongly recommended that you do not update VIA Switches and connected PoE devices at the same time. It is possible for the firmware update process to reboot the Switch before the data has finished writing to the PoE devices' memory. If the VIA Switch reboots at this point, the connected PoE devices'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

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




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

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

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

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

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

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

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

The device will then reboot, having reset itself to the Factory settings. Before configuration can be restored, the unit must be secured (either by adding to a Security Domain, or enabling Local Security).

FRONT PANEL LOCKOUT

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

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

FRONT PANEL UI AND MENU

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

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

BEFORE YOU START

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

You will need to secure the device in some manner before you are able to configure the device. The device must be either **Locally Secured** or it must be added to a **Security Domain using Pathscape** (see earlier Security section).

If **Locally Secured**, some functionality will not be available such as Pathway ssACN. Pathway ssACN needs the device to be part of a Domain in order to authenticate and send traffic; if **Locally Secured** the device is essentially in a Domain by itself, so it cannot send any data using that protocol.

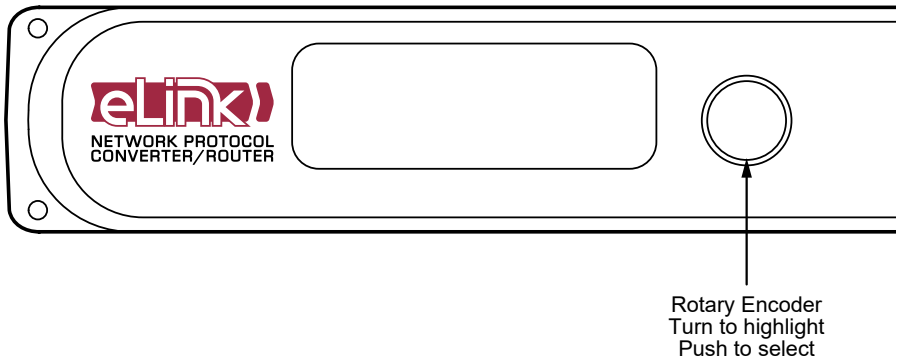
Non-standard Universes (Custom Patches) can only be edited and assigned to Paths using Pathscape.

If you must use the device without Pathscape, you must **Locally Secure** it 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 secure access to your network, both physically and technologically. To continue, you must acknowledge that you have read this statement and accept these risks.

FRONT PANEL UI



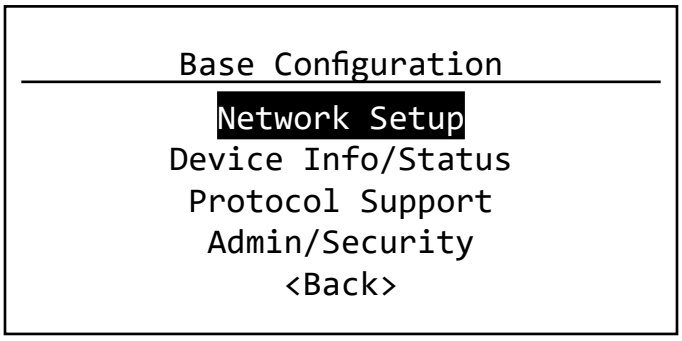
MAIN DISPLAY MESSAGES

When idle, the main LCD will show the device soft label (Name) and its IP address. When the device has an active network connection, the flashing icon will be shown at the bottom of the LCD.

If the device is not locally secured or on a Security Domain, the main menu will say "**Device Must be Secured**" on the bottom line.

USING THE FRONT PANEL UI

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



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

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

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

FRONT PANEL LOCKOUT

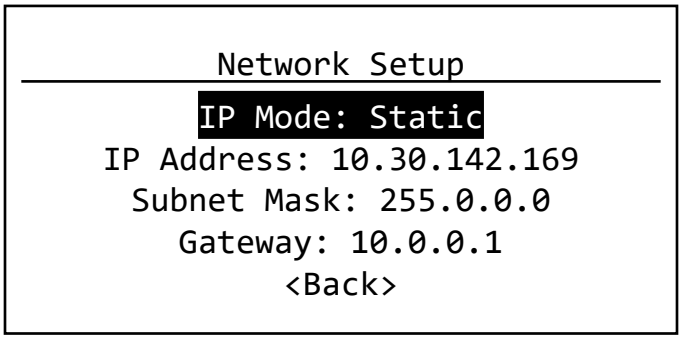
If using Pathscape, it is possible to enable the option **Front Panel Lockout**, which disables the ability to make any changes to the device from the front panel UI. You can still navigate the menus to review settings, but cannot change any properties.

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

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

MENUS

NETWORK SETUP



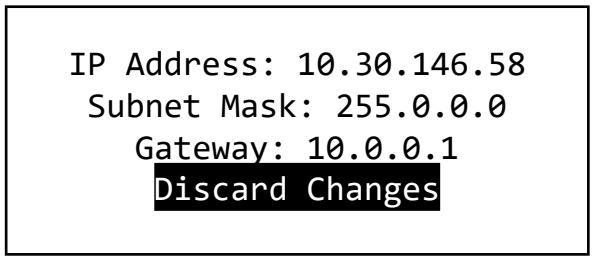
This menu allows review and changes to the device IP mode, IP address, subnet mask, and default gateway. Scroll the encoder knob to highlight the property you want to edit, and push the knob to edit the value. Scroll the knob again to choose the new value, and push the knob to confirm.

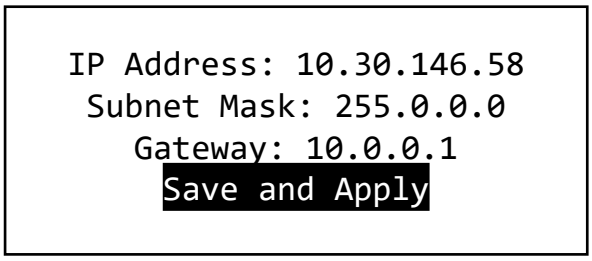
Depending on the item you are editing, you may have to scroll down to select the **<Back>** option to return to the previous menu, or select **Save and Apply** to confirm. In some menus you may also select **Discard Changes** to return to the previous menu without committing changes.

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

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

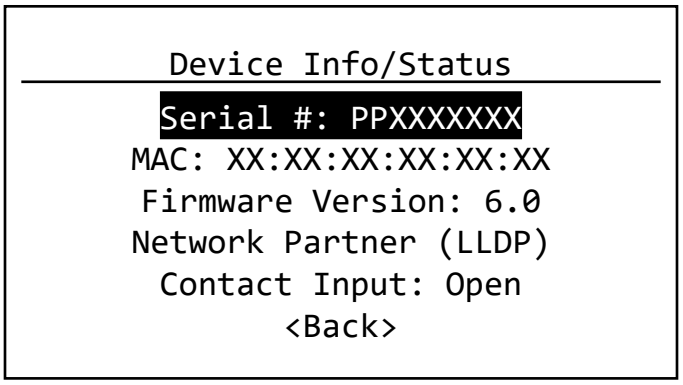
Once the values have been set, acceptance options appear on the bottom line of the screen. By default, **Discard Changes** will be highlighted. Click the knob to cancel and return to previous menu. Turn the knob to select **Save and Apply** to save changes and return to the **Network Setup** menu.





DEVICE INFO/STATUS

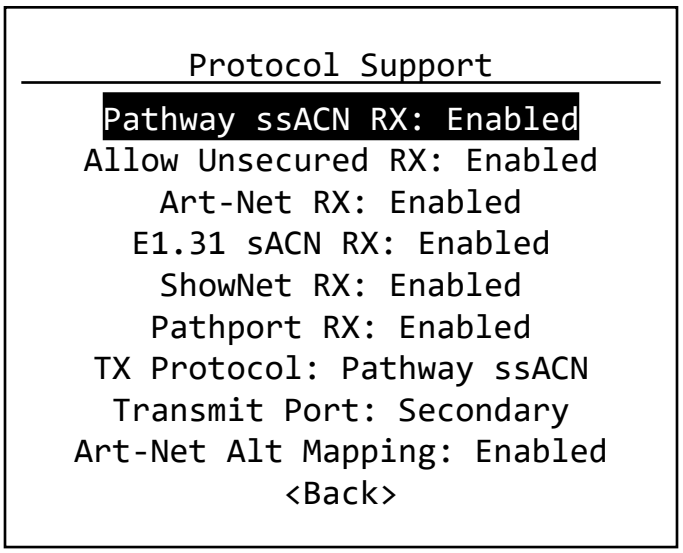
This menu allows review of several device properties. These are read-only.



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

PROTOCOL SUPPORT

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



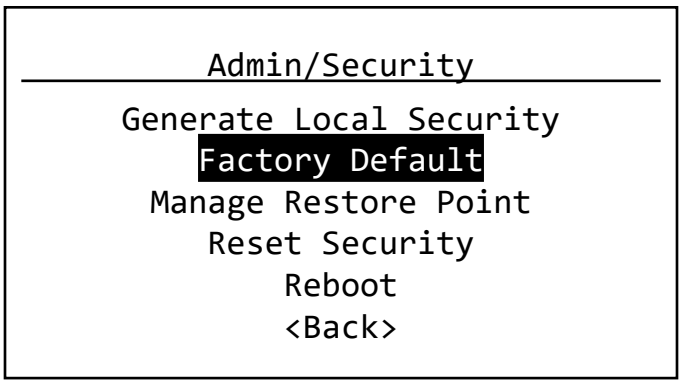
The above menu is laid out in a manner that reflects the property locations in the Pathscape Properties pane as close as possible. Note that some property names are shortened in order to fit on the LCD screen.

Menu Item	Description
Pathway ssACN RX:	**Enable** (default) or **Disable** receiving of Pathway ssACN.
Allow Unsecured RX	**Enable** or **Disable** (default) the receiving of unsecured Network DMX Protocols.
Art-Net RX	**Enable** or **Disable** (default) the receiving of Art-Net. If **Allow Unsecured RX** is set to Disabled, this menu item will be hidden.
E1.31 sACN RX	**Enable** or **Disable** (default) the receiving of E1.31 sACN. If **Allow Unsecured RX** is Disabled, this menu item will be hidden.
ShowNet RX	**Enable** or **Disable** (default) the receiving of Strand ShowNet. If **Allow Unsecured RX** is Disabled, this menu item will be hidden.
Pathport RX	**Enable** or **Disable** (default) the receiving of Pathport Protocol. If **Allow Unsecured RX** is Disabled, this menu item will be hidden.

Menu Item	Description
TX Protocol	Select the Network DMX protocol the eLink should use when transmitting. Options are: **Pathport**: Use Pathway Pathport protocol **Art-Net**: Use Art-Net protocol **ShowNet**: Use Strand ShowNet protocol **E1.31sACN**: Use standard E1.31 sACN protocol **Pathway ssACN** (default): Use Pathway ssACN protocol <Back>: Return to previous menu.
Transmit Port	Select whether the eLink should transmit the Path outputs on the Secondary Ethernet port only, or on Both the Primary & Secondary Ports.
Art-Net Alt Mapping	When enabled, Art-Net Universe 0:0 is treated as Universe 1. When disabled, Art-Net universe 0:0 is ignored and Art-Net Universe 1 is the same as Pathscape Universe 1. Select whether Art-Net Alternate Mapping is **enabled** (default) or **disabled**.
<Back>	Return to previous menu.

ADMIN/SECURITY

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

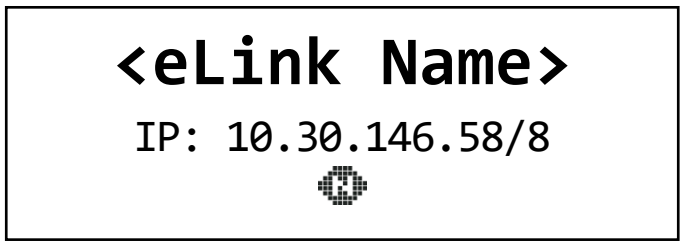


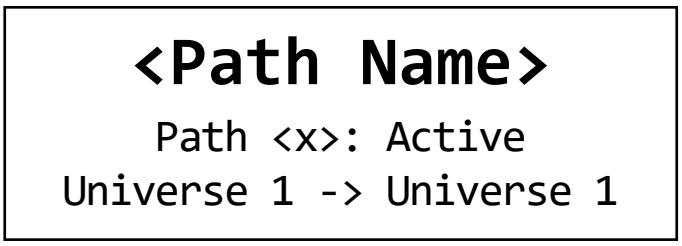
Menu Item	Description
Generate Local Security	**Will appear only when device is not secured,** e.g. when powered on for the first time, or after being factory defaulted or after having security settings reset. Selecting this will generate local security for the device. You will be able configure the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

Menu Item	Description
Manage Restore Point	Allows you to create, update or recall the Device Restore Point. A Device Restore Point is a saved copy of all device settings, allowing you to restore the device back to a known state or preferred configuration at any time. Note that there can only be one restore point on a device at a time. **Create**: Saves a new restore point if none already exists, copying all the device's current settings. **Update**: Overwrites the existing restore point with the device's current settings. **Recall**: Recalls the restore point and overwrites the current device settings with those saved in the restore point. <Back>: Return to previous menu.
Reset Security	**Will only be shown if the device is secured.** Allows you to reset the device's security settings without affecting the rest of the device configuration. This is analogous to removing the device from the Security Domain using Pathscape. After selecting this menu item you will be asked to **confirm** your decision.
Reboot	Will cause the device to soft reboot. After selecting this menu item you will be asked to **confirm** your decision.
<Back>	Return to previous menu.

PATH STATUS AND CONFIGURATION MENU

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





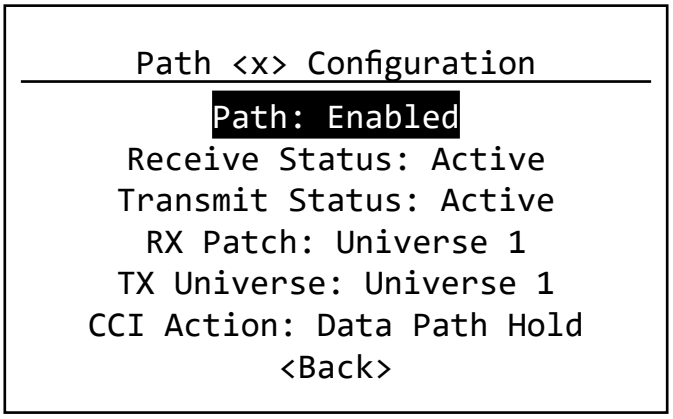
The Path's soft label, configurable in Pathscape, is shown on the top line. By default, the label is the Path number.

Below that, the Path number and status is shown. The status value will be:

- **Disabled** (Path is disabled either in Pathscape or in the menu below)
- **Inactive** (Path is not transmitting any data)
- **Active** (Path is transmitting data)

The bottom line shows the RX Patch and the TX Universe of selected Path.

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



Menu Item	Description
Path	For debugging purposes or otherwise, you may want to disable an eLink Network Path. All other properties will remain unchanged. Choose **Enabled** (default) or **Disabled.** <Back>: Return to previous menu.
Receive Status	Shows status of the Network DMX source for this Path. Will show **Active** when Network DMX stream is present, and **Inactive** if Network DMX stream is lost. Read-only.

Menu Item	Description
Transmit Status	Shows status of the Network DMX output of this Path. Will show **Active** when Network DMX stream is being output and **Inactive** if no Network DMX is being output. Read-only. **NOTE**: In situations where source signal is lost, depending on signal loss settings, it is possible for the Network DMX TX to be Active while the Network DMX RX is Inactive.
RX Patch:	Shows and allows selection of the RX Patch for the selected Path. Scroll the list to choose from standard Universes, from 1 to 63999. If you have previously set a **Custom RX Patch** using Pathscape, its name will be shown here. **NOTE** that you cannot select or create Custom RX Patches using the front panel. If you select a standard Universe, you will not be able to select the previously used Custom RX Patch again from the front panel, it will need to be set using Pathscape. <Back>: Return to previous menu.
TX Universe:	Shows and allows selection of the TX Universe for the selected Path. Scroll the list to choose from standard Universes, from 1 to 63999. <Back>: Return to previous menu.
CCI Action	Shows and allows selection of the Contact Closure Interface action. **None** (default): CCI does nothing. **Data Path Hold**: CCI will force the eLink Path output to snapshot the current receive levels and maintain them indefinitely, ignoring any further changes. Useful to lock out any unintended changes once levels are set as desired. <Back>: Return to previous menu.
<Back>	Return to previous menu.

APPENDIX 1: ELECTRICAL, COMPLIANCE & OTHER INFORMATION

ELECTRICAL INFORMATION

- Power input:
  - Power-over-Ethernet (PoE): Class 1 Device, 4.2W Maximum draw
  - Auxiliary DC input: 24-48VDC, 175 mA Maximum current draw

COMPLIANCE

- ANSI E1.31 sACN - Streaming ACN, Art-Net, Strand ShowNet, Pathway ssACN
- IEEE 802.3af - Class 2 Power-over-Ethernet (PoE)
- California Title 1.81.26, Security of Connected Devices
- RoHS 2011/65/EU + A1 2015/863
- CE

PHYSICAL

- Weight: 2.3 lbs (1kg) [base device, without attached rack mounting hardware]
- Dimensions: 8.6” W x 1.7” H x 7” D (218mm W x 43mm H x 178mm D) [base device, without attached rack mounting hardware]
- Operating Conditions: 32°F to 122°F (0°C to 50°C); 5-95% relative humidity, non-condensing