DIN-mount Ethernet Switches

PWVIA DIN Models

Running firmware 6.X or later

User Guide

March 2022

© 2022 Acuity Brands, Inc. • One Lithonia Way, Conyers GA 30012
Pathway Connectivity | #103 - 1439 17th Ave SE Calgary, AB Canada T2G 1J9
Phone: + 1 866 617 3074

WARNING ABOUT INSECURE 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 VIA DIN-MOUNT ETHERNET SWITCHES - PWVIA DIN

PWVIA Ethernet Switches are designed for live entertainment Ethernet systems, including audio, video and DMX-over-Ethernet networks. This manual covers models **PWVIA DIN P16 and PWVIA DIN P8 models**.

VIA Ethernet Switches are intended specifically for signal routing between Pathport DMX-over-Ethernet gateways, or similar equipment, and Ethernet-aware lighting and audio control products, such as consoles and controllers and end equipment. A VIA is a routing device and is not a source of the control protocols or the data being passed. Switches only provide management control over the data path.

The VIA family is easily configured and upgraded using the freely available software tool, **Pathscape**.

INSTALLATION INSTRUCTIONS

The PWVIA DIN P16 and PWVIA DIN P8 switches are DIN-mountable and intended for use in NEMA enclosures, or to be mounted in a standard 19” equipment rack, using the PWENC SHELF HOR 2-Rack Shelf Unit.

All PWVIA DIN Switches are intended for installation in a dry, indoor location. Ambient operating conditions are **14°F to 113°F (-10°C to 45°C); 5-95% relative humidity, non-condensing.**

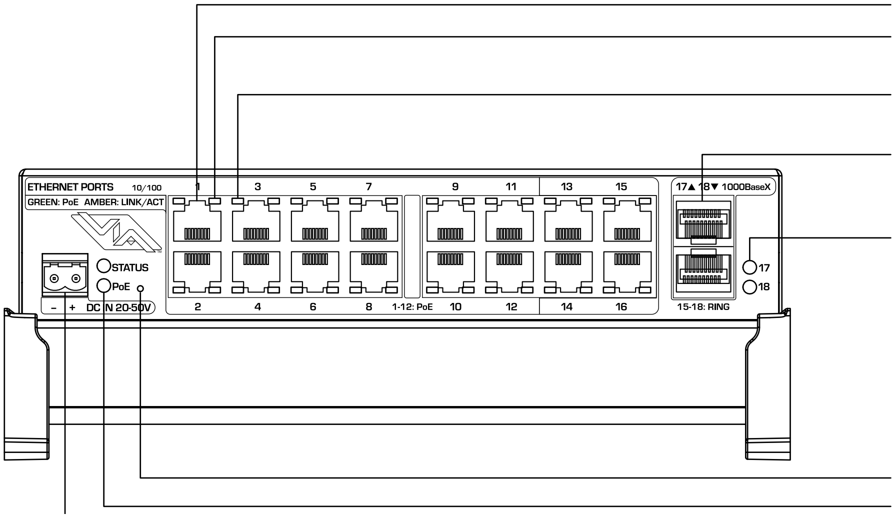
Warning: This equipment relies on building installation primary overcurrent protection.

Warning: All ports on the PWVIA DIN P16 and PWVIA DIN P8 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

MODEL PWVIA DIN P16 RJ45 SFPSLOT POE



Female 10/100 RJ45 connectors (x16)

Amber LED (Link Active)

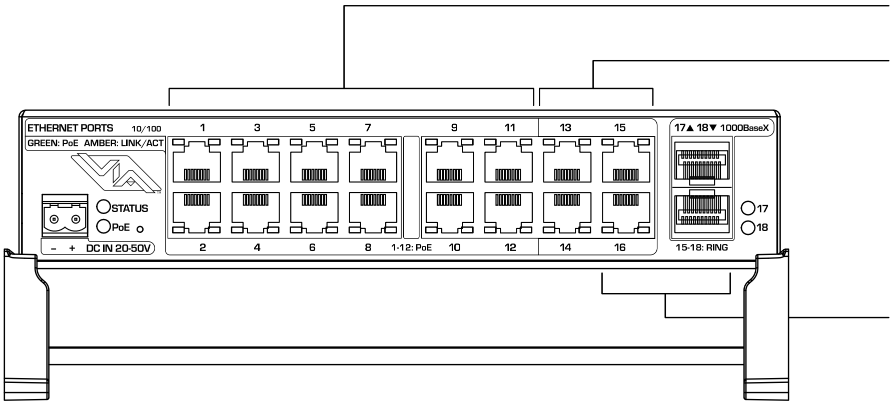
Green LED (PoE Active)

2x SFP Ports for Fiber transceivers or copper direct-attach cables

Link/Status LEDs indicators for fiber ports

Factory Reset button (recessed)

Processor Status and PoE LED indicators



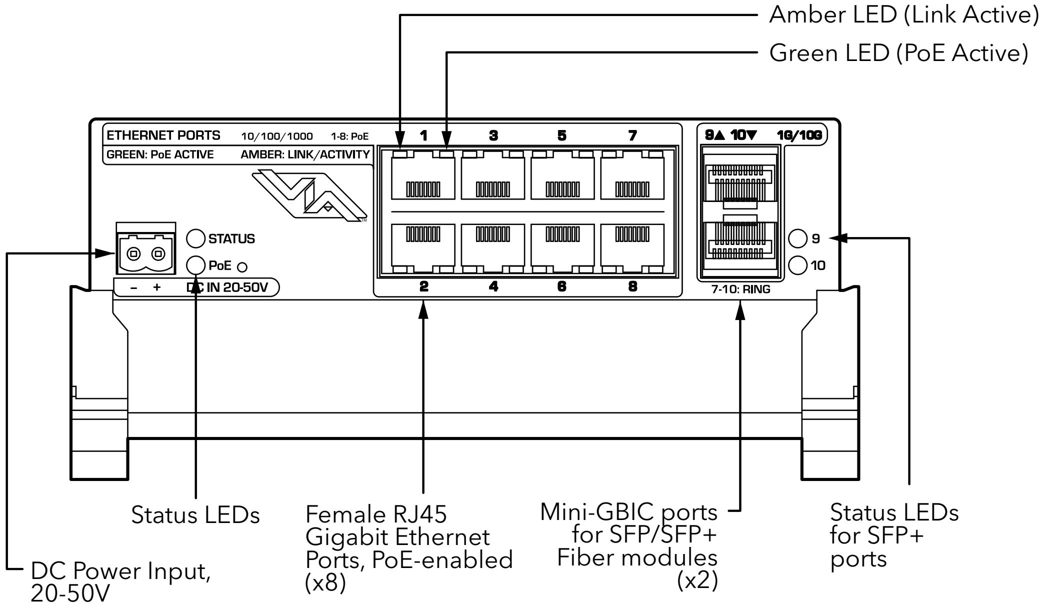
PoE-enabled ports (1-12)

Non-PoE Ports (13-16)

Ethernet ports are numbered
top to bottom, left to right.
Top row: 1, 3, 5, 7, 9, 11, 13, 15
Bottom row: 2, 4, 6, 8, 10, 12, 14, 16

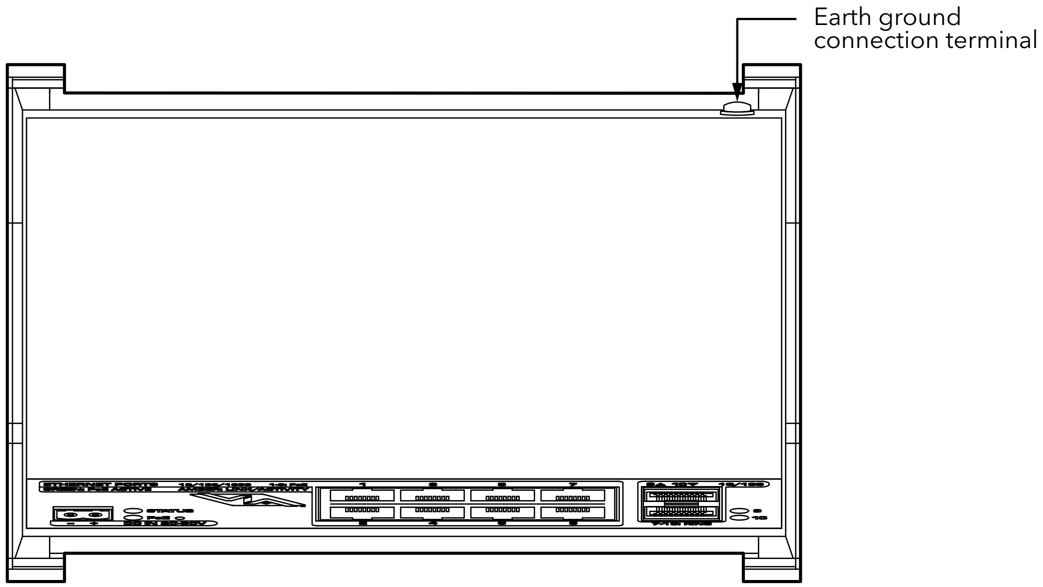
EAPS Ring Protect-enabled ports (Ethernet ports 15-16 and Fiber ports 17-18)

MODEL PWVIA DIN P8 RJ45 SFPSLOT POE



REAR PANEL

MODEL PWVIA DIN P16 RJ45 SFPSLOT POE, PWVIA DIN P8 RJ45 SFPSLOT POE



RJ45 ETHERNET PORTS

The **PWVIA DIN P16** has 16 female RJ45 Ethernet ports on the front panel. These are 10/100 Mbit. The first 12 of these support Class 3 Power-over-Ethernet (PoE); the last 4 **do not**.

The **PWVIA DIN P8** has 8 female RJ45 Ethernet ports on the front panel. These are 1Gbit. All 8 ports support Class 3 Power-over-Ethernet (PoE).

Each RJ45 port has two LEDs. The green LED (left-side) will show PoE activity. The amber LED (right-side) will show Link activity.

SFP PORTS

The PWVIA DIN P16 has two SFP compatible ports (ports 17-18). These require the user to provide an SFP fiber transceiver to allow connection to fiber networks. See **Appendix 1: SFP/SFP+ Fiber Adapter Selection** for more information on selecting a fiber transceiver.

SFP+ PORTS

The PWVIA DIN P8 has two SFP+ compatible ports (ports 9-10). These require the user to provide an SFP+ fiber transceiver to allow connection to fiber networks. See **Appendix 1: SFP/SFP+ Fiber Adapter Selection** for more information on selecting a fiber transceiver.

The user may also use SFP+ Direct Attach cables, both active and passive. This is often the easiet and lowest-cost way to connect multiple switches together, if they are close together in the same enclosure or rack.

POWER CONNECTIONS

The **DC IN** jack must be connected to an external power supplying at minimum 20 VDC to power the switch. If you are intending to use the PWVIA DIN P16 or PWVIA DIN P8 as a PoE source, the external power supply must provide 48-50 VDC with enough watts to satisfy the draw of connected equipment.

Class 3 PoE (15.4 W) is available on the first 12 Ethernet ports on the PWVIA DIN P16. All 8 ports on the PWVIA DIN P8 can supply PoE.

If you intend on using Class 3 devices on all the 12 ports of the PWVIA DIN P16, the external supply must be 200 Watts. If you intend on using Class 3 devices on all 8 ports of the PWVIA DIN P8, the external supply must be 150 Watts.

If you are using lower-power devices such as Pathport gateways and Vignette or NSB stations, you may use a smaller supply. For a typical configuration with mostly Class 2 or lower devices, a 100W 48VDC supply (P/N 1001-100-48-DIN) will be sufficient. Always ensure your supply has enough power to supply your connected devices, and set the **PoE External Supply Power** property for the switch appropriately in Pathscape.

CONFIGURATION

All configuration of the PWVIA DIN P16 and PWVIA DIN P8 must be done with the 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.

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 and later, 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.

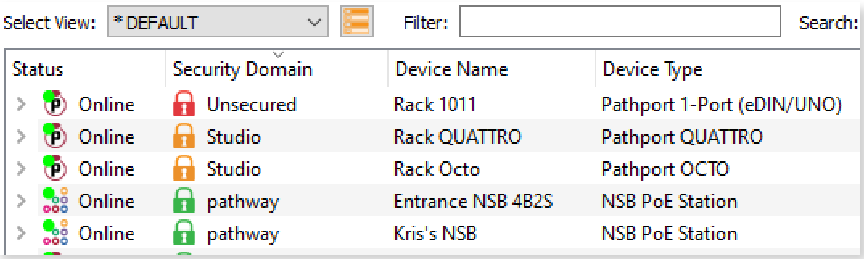
8. The complete network configuration may be saved without a password before factory defaulting devices. Applying the saved configuration will require a new password to be set for the network.

9. Configuring our devices to receive unsecured protocols such as sACN and ArtNet 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) introduced the concept of a “**Security Domain**”. Below we will describe how to create a Security Domain and add or remove devices from it. In the **Device** tab of Pathscape there is a view that shows you the name of the device’s domain and a **padlock icon** showing its current state.



Select View: * DEFAULT   Filter: Search:

Status	Security Domain	Device Name	Device Type
Online	🔒 Unsecured	Rack 1011	Pathport 1-Port (eDIN/UNO)
Online	🔒 Studio	Rack QUATTRO	Pathport QUATTRO
Online	🔒 Studio	Rack Octo	Pathport OCTO
Online	🔒 pathway	Entrance NSB 4B2S	NSB PoE Station
Online	🔒 pathway	Kris's NSB	NSB PoE Station

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

AMBER PADLOCK - 🔒 Secured Device not in the Current Domain

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

AMBER PADLOCK - 🔒 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 or Reset Security settings** from the front panel and add it to the Security Domain using Pathscape.

GREEN PADLOCK - 🔒 Secured Device in Current Domain

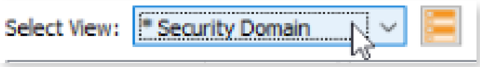
Once you have logged into a Security Domain with a password, any device in your domain will appear with a green padlock and all their properties will be Read/Writeable.

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

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

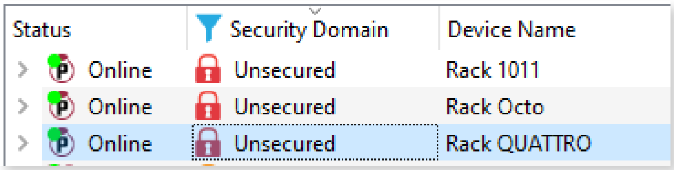
CREATING A SECURITY DOMAIN

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



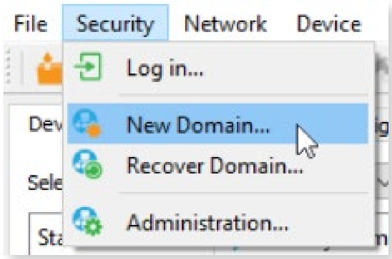
Select View: Security Domain

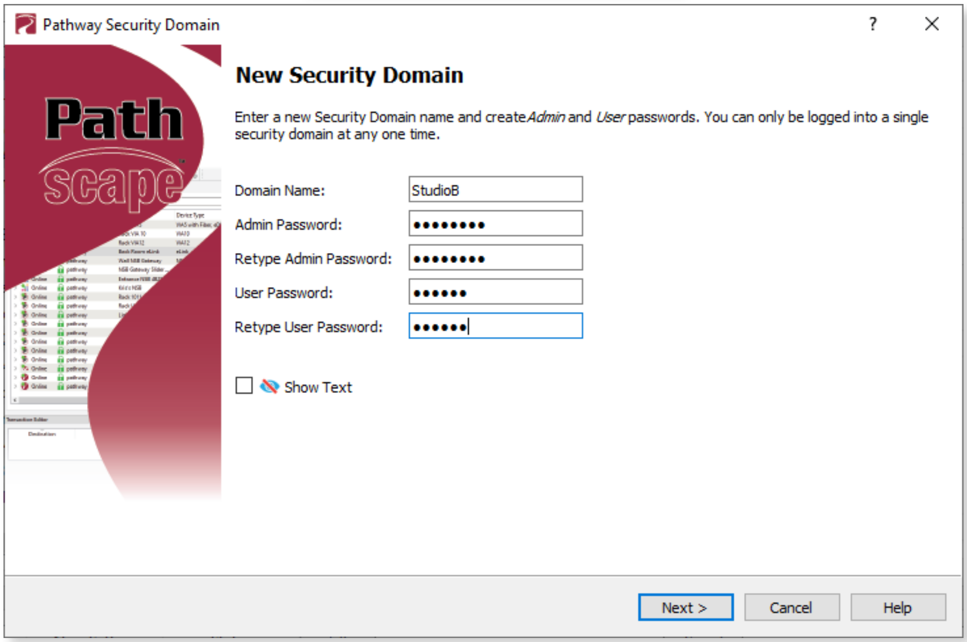
- Each device running V5 or later firmware will have a **Red "Unsecured"** value in the **Security Domain** column.



Status	Security Domain	Device Name
Online	Unsecured	Rack 1011
Online	Unsecured	Rack Octo
Online	Unsecured	Rack QUATTRO

- (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.**





Pathway Security Domain

New Security Domain

Enter a new Security Domain name and create *Admin* and *User* passwords. You can only be logged into a single security domain at any one time.

Domain Name: StudioB

Admin Password: ••••••••

Retype Admin Password: ••••••••

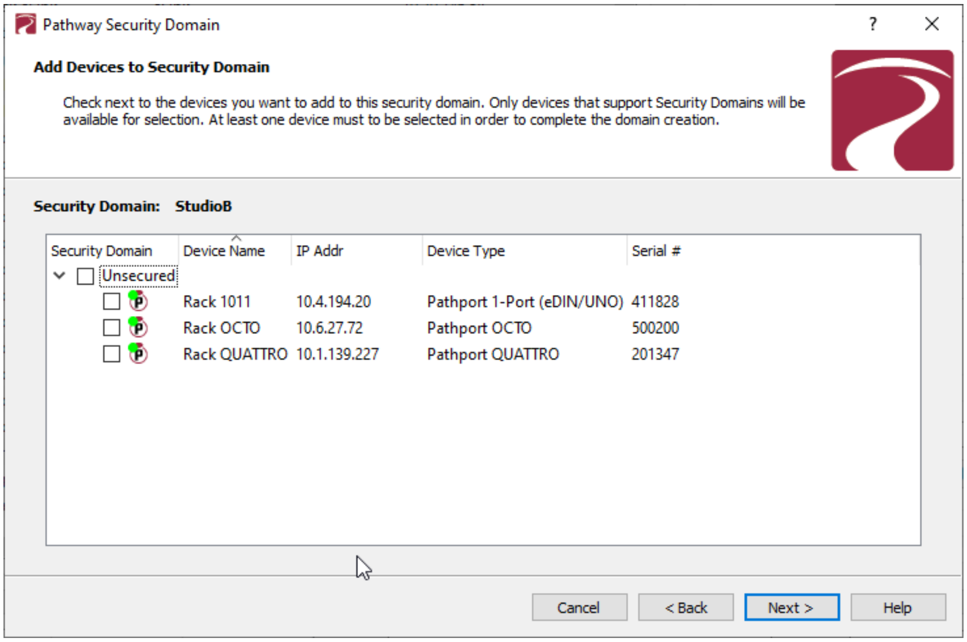
User Password: ••••••

Retype User Password: ••••••

☐ Show Text

- 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 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.



Pathway Security Domain

Add Devices to Security Domain

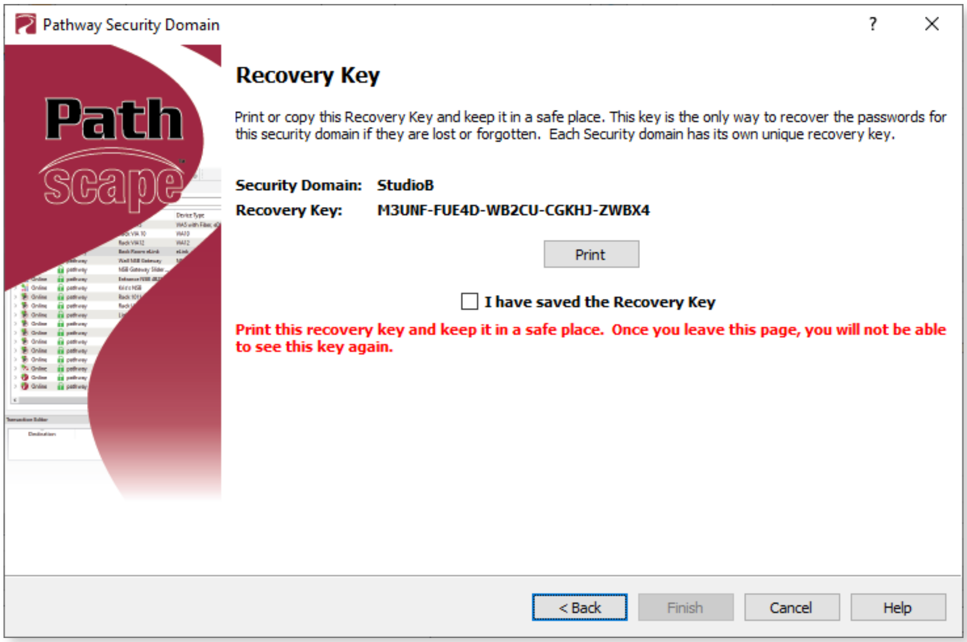
Check next to the devices you want to add to this security domain. Only devices that support Security Domains will be available for selection. At least one device must to be selected in order to complete the domain creation.

Security Domain: StudioB

Security Domain	Device Name	IP Addr	Device Type	Serial #
□ Unsecured				
□	Rack 1011	10.4.194.20	Pathport 1-Port (eDIN/UNO)	411828
□	Rack OCTO	10.6.27.72	Pathport OCTO	500200
□	Rack QUATTRO	10.1.139.227	Pathport QUATTRO	201347

- 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.



Pathway Security Domain

Recovery Key

Print or copy this Recovery Key and keep it in a safe place. This key is the only way to recover the passwords for this security domain if they are lost or forgotten. Each Security domain has its own unique recovery key.

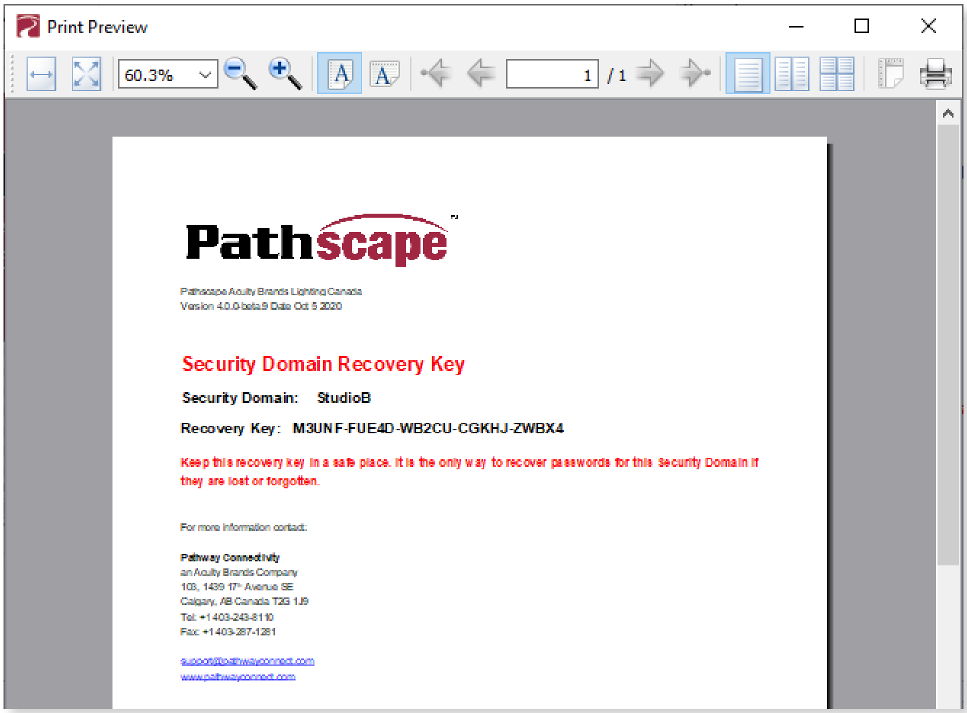
Security Domain: StudioB

Recovery Key: M3UNF-FUE4D-WB2CU-CGKHJ-ZWBX4

□ I have saved the Recovery Key

Print this recovery key and keep it in a safe place. Once you leave this page, you will not be able to see this key again.

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



Pathscape™

Pathscape Acuity Brands Lighting Canada
Version 4.0.0-beta.9 Date Oct 5 2020

Security Domain Recovery Key

Security Domain: StudioB

Recovery Key: M3UNF-FUE4D-WB2CU-CGKHJ-ZWBX4

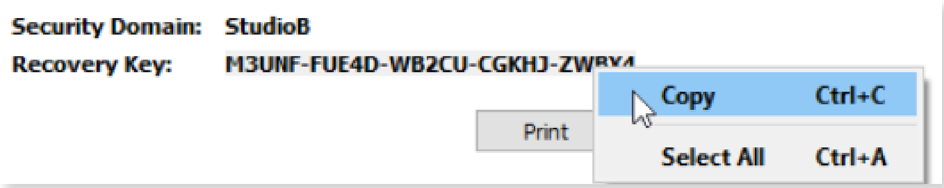
Keep this recovery key in a safe place. It is the only way to recover passwords for this Security Domain if they are lost or forgotten.

For more information contact:

Pathway Connectivity
an Acuity Brands Company
103, 1439 17th Avenue SE
Calgary, AB Canada T2G 1J9
Tel: +1 403-243-8110
Fax: +1 403-287-1281

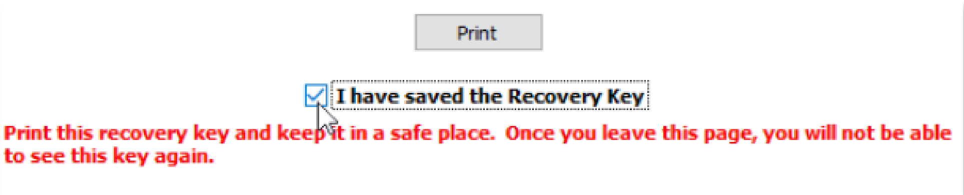
support@pathwayconnect.com
www.pathwayconnect.com

- 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.



Security Domain: StudioB
Recovery Key: M3UNF-FUE4D-WB2CU-CGKHJ-ZWBX4

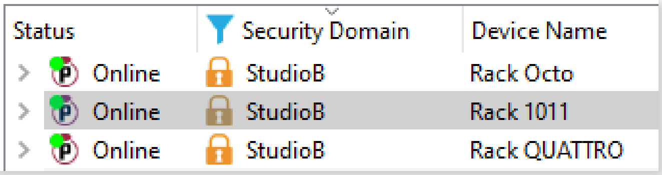
- In order to proceed, you **must click the checkbox** acknowledging you have printed or saved the Recovery Key in some way.



☑ I have saved the Recovery Key

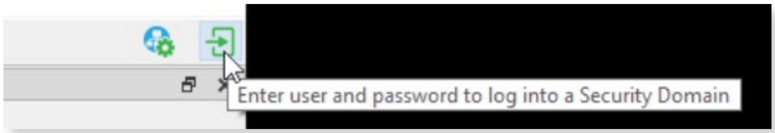
Print this recovery key and keep it in a safe place. Once you leave this page, you will not be able to see this key again.

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



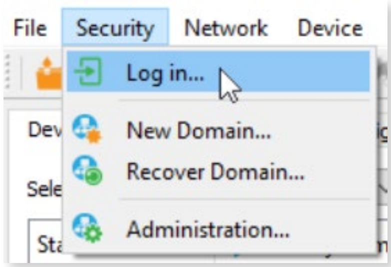
Status	Security Domain	Device Name
Online	StudioB	Rack Octo
Online	StudioB	Rack 1011
Online	StudioB	Rack QUATTRO

- 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

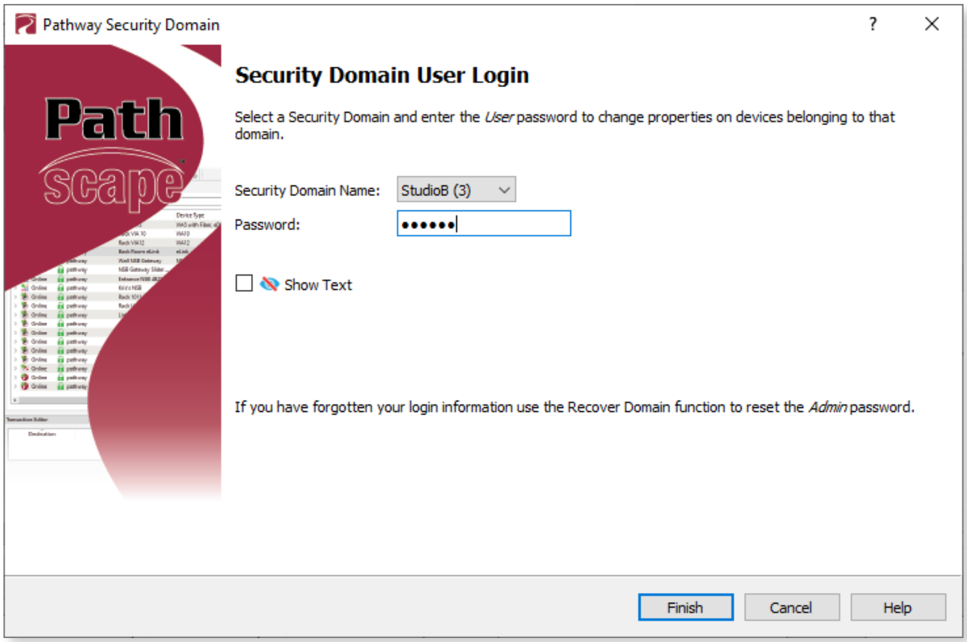


Enter user and password to log into a Security Domain

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**.



Pathway Security Domain

Security Domain User Login

Select a Security Domain and enter the *User* password to change properties on devices belonging to that domain.

Security Domain Name: StudioB (3)

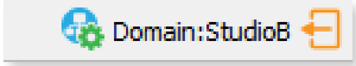
Password: ••••••

□ Show Text

If you have forgotten your login information use the Recover Domain function to reset the *Admin* password.

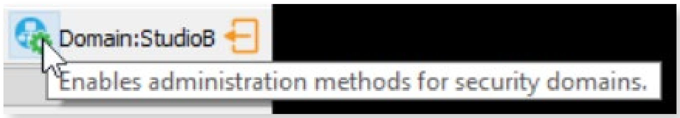
As security parameters are verified, the amber padlocks will turn green and the properties of those devices will be read/writable.

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.

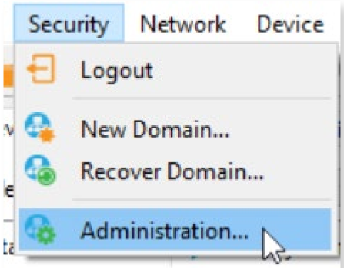


ADMINISTERING A DOMAIN

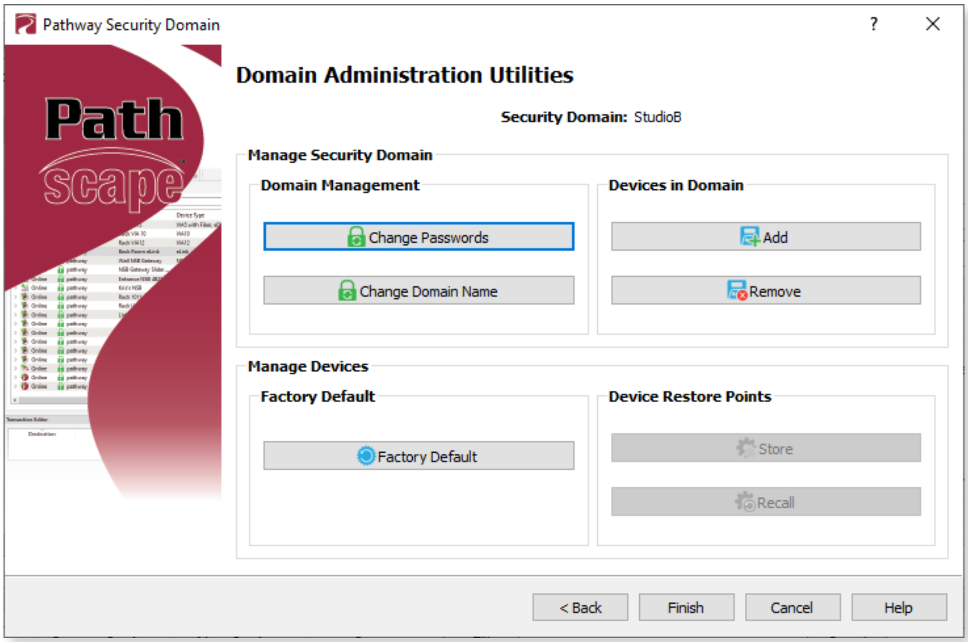
To administer a domain, click on the **Administration** button on the Security Toolbar, or click the **Security** menu and select **Administration**.



Enables administration methods for security domains.



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

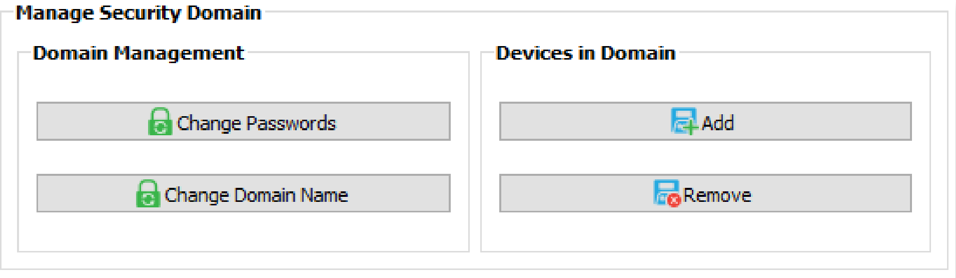


Security Domain: StudioB

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

MANAGE SECURITY DOMAIN

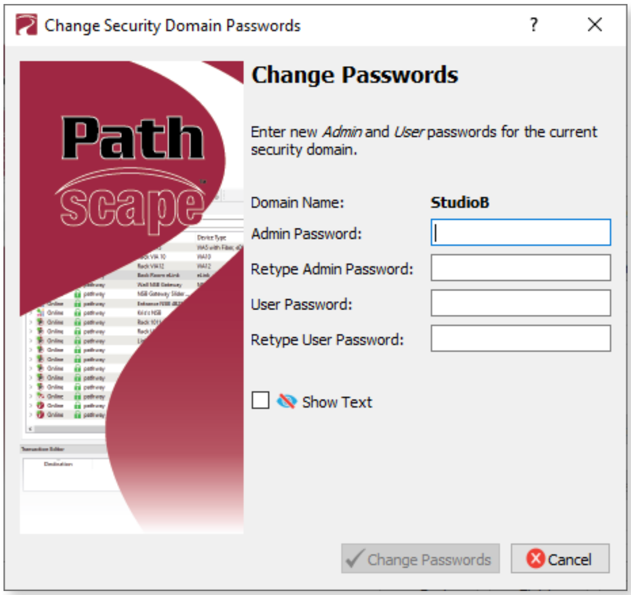
This section is broken down further into functions that relate to **Domain Management**, including Domain Name and Passwords, and **Devices in Domain**, which allows you to add and remove devices in the Domain.



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.**



Change Security Domain Passwords

Change Passwords

Enter new *Admin* and *User* passwords for the current security domain.

Domain Name: **StudioB**

Admin Password:

Retype Admin Password:

User Password:

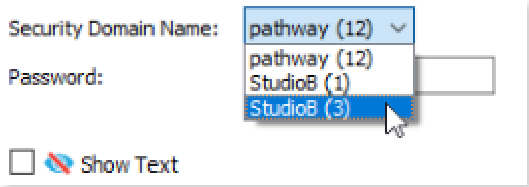
Retype User Password:

□ Show Text

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 the old password. When logging in, there will be two domains with the same name.



Security Domain Name: pathway (12)

Password:

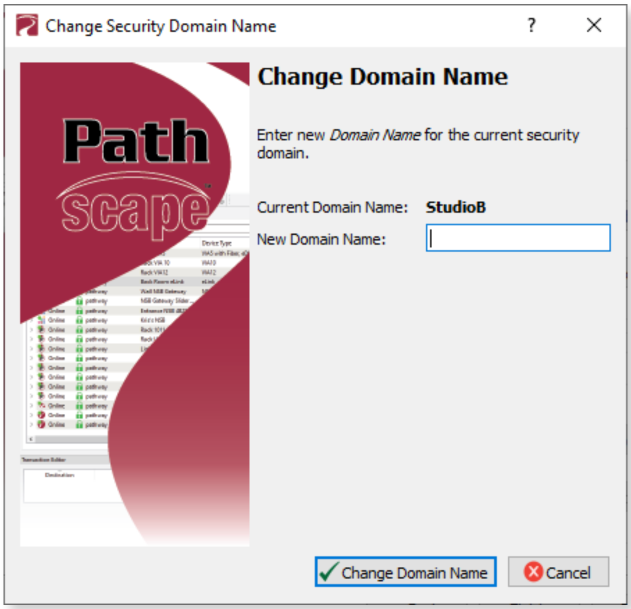
□ Show Text

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.



Change Domain Name

Enter new *Domain Name* for the current security domain.

Current Domain Name: **StudioB**

New Domain Name:

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

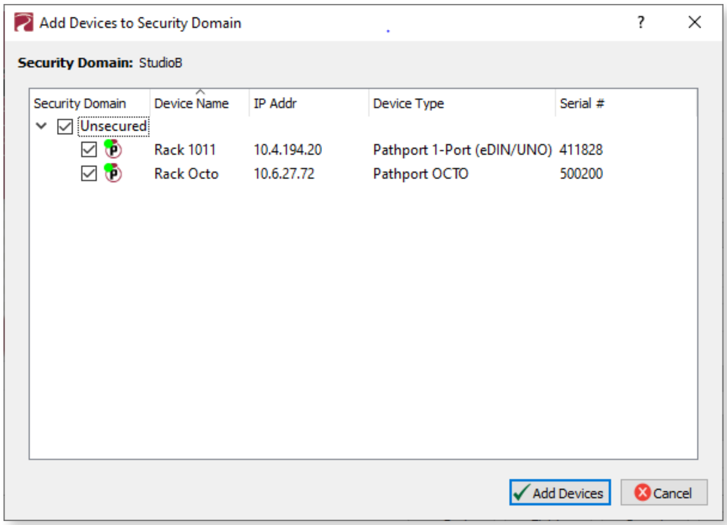
The window will close, and you will be logged out of the current domain, and the Domain Name will be changed to the new value. **You will have to log into the Domain again** to make any further changes.

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.



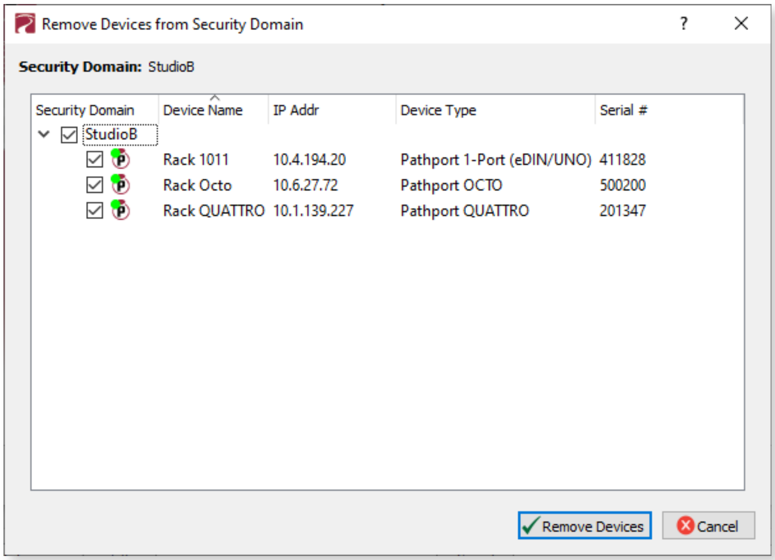
Security Domain: StudioB

Security Domain	Device Name	IP Addr	Device Type	Serial #
☑ Unsecured				
☑	Rack 1011	10.4.194.20	Pathport 1-Port (eDIN/UNO)	411828
☑	Rack Octo	10.6.27.72	Pathport OCTO	500200

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.



Security Domain: StudioB

Security Domain	Device Name	IP Addr	Device Type	Serial #
☑ StudioB				
☑	Rack 1011	10.4.194.20	Pathport 1-Port (eDIN/UNO)	411828
☑	Rack Octo	10.6.27.72	Pathport OCTO	500200
☑	Rack QUATTRO	10.1.139.227	Pathport QUATTRO	201347

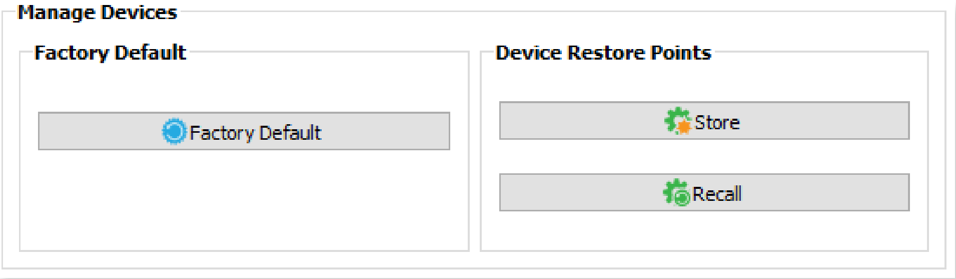
Click on the checkboxes next to the devices you want to remove from the Domain, and click the **Remove Devices** button. To remove all the listed devices, click the top checkbox next to the Domain Name which will auto-check all the devices' checkboxes.

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**.



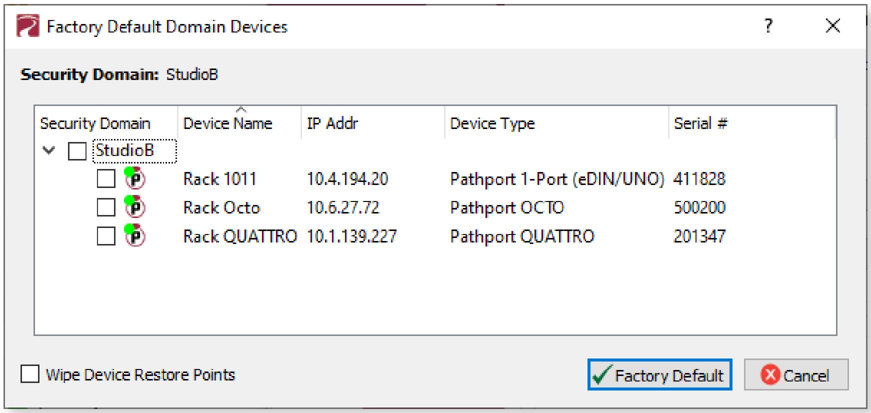
FACTORY DEFAULT

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.


Factory Default Domain Devices

Security Domain: StudioB

Security Domain	Device Name	IP Addr	Device Type	Serial #
☐ StudioB				
☐	Rack 1011	10.4.194.20	Pathport 1-Port (eDIN/UNO)	411828
☐	Rack Octo	10.6.27.72	Pathport OCTO	500200
☐	Rack QUATTRO	10.1.139.227	Pathport QUATTRO	201347

☐ Wipe Device Restore Points

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.

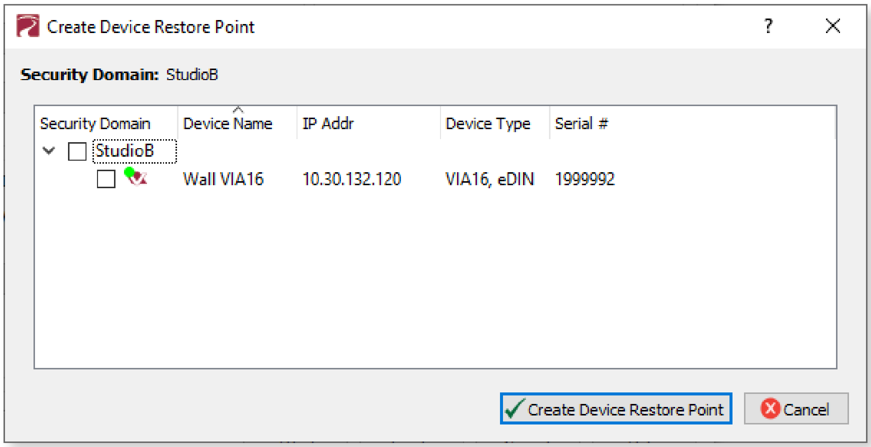
DEVICE RESTORE POINTS

With the release of firmware V6.0, VIA Switches including models PWVIA RM P12, PWVIA DIN P16, and PWVIA DIN P8 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.



Security Domain: StudioB

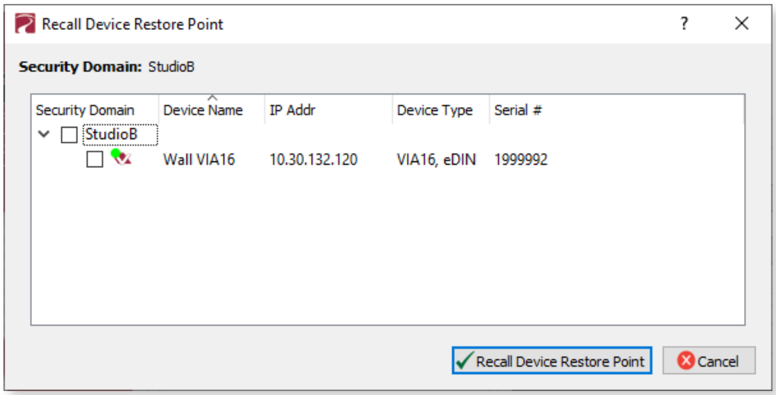
Security Domain	Device Name	IP Addr	Device Type	Serial #
□ StudioB				
□	Wall VIA16	10.30.132.120	VIA16, eDIN	1999992

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 greyed out.

RECALL

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



Security Domain: StudioB

Security Domain	Device Name	IP Addr	Device Type	Serial #
□ StudioB				
□	Wall VIA16	10.30.132.120	VIA16, eDIN	1999992

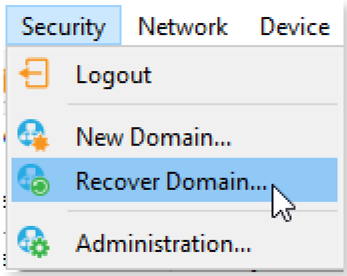
Click the checkbox next to each device on which you'd like to recall its restore point. To check all devices, click the topmost checkbox. Click **Recall Device Restore Point** to confirm.

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

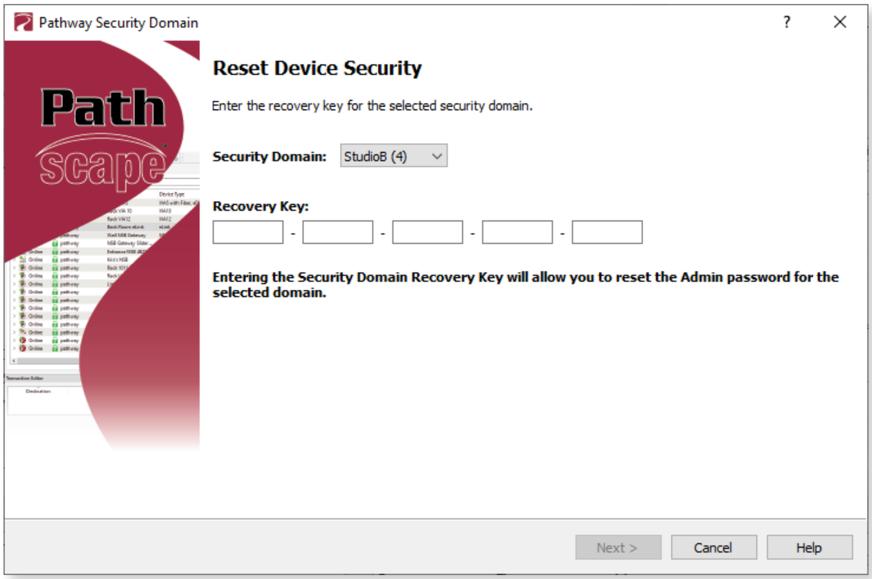
RECOVERING A DOMAIN

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

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



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



Reset Device Security

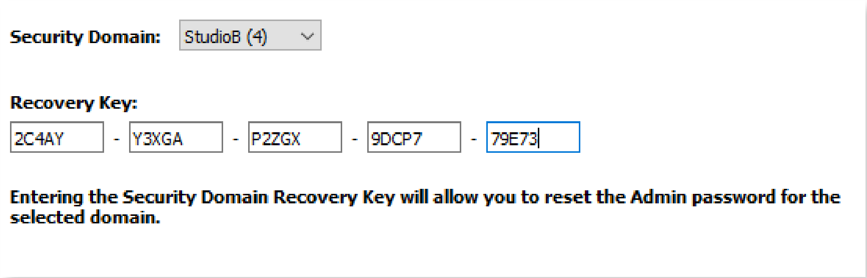
Enter the recovery key for the selected security domain.

Security Domain: StudioB (4)

Recovery Key:

Entering the Security Domain Recovery Key will allow you to reset the Admin password for the selected domain.

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



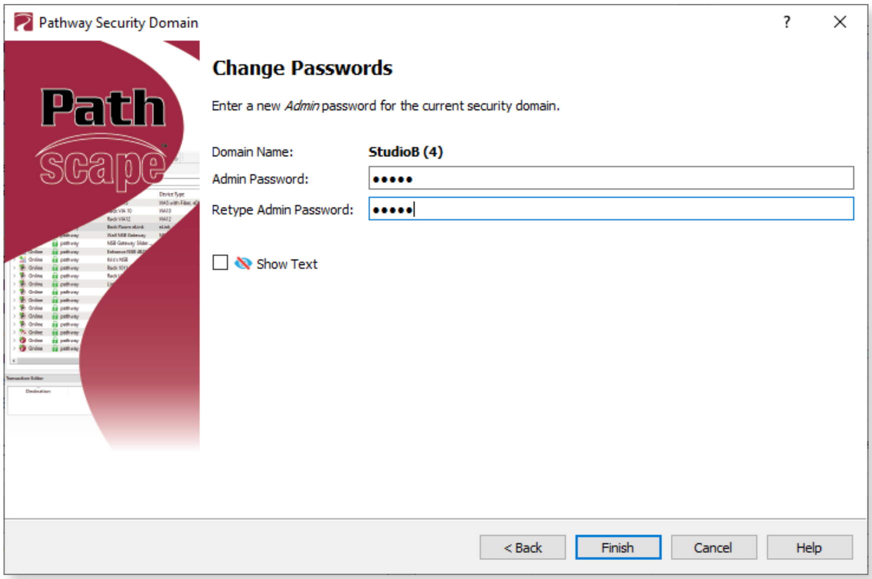
Security Domain: StudioB (4)

Recovery Key:

2C4AY - Y3XGA - P2ZGX - 9DCP7 - 79E73

Entering the Security Domain Recovery Key will allow you to reset the Admin password for the selected domain.

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



Pathway Security Domain

Change Passwords

Enter a new *Admin* password for the current security domain.

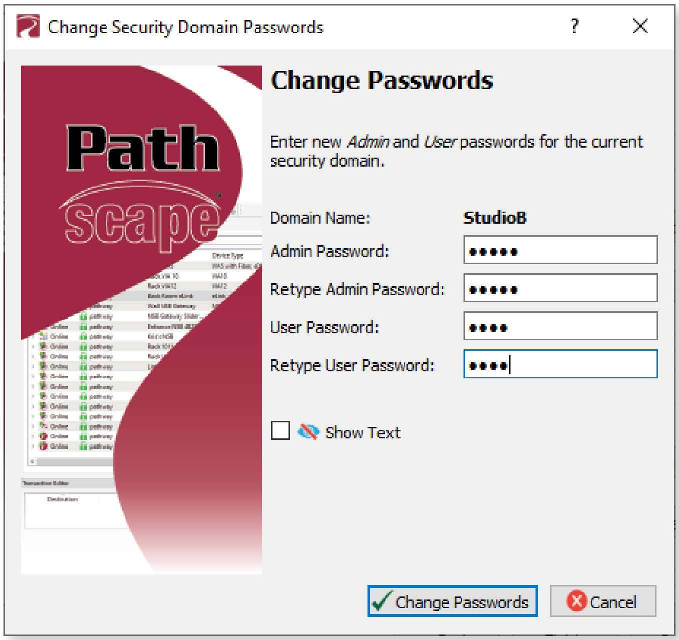
Domain Name: **StudioB (4)**

Admin Password: •••••

Retype Admin Password: •••••

□ Show Text

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



Change Security Domain Passwords

Change Passwords

Enter new *Admin* and *User* passwords for the current security domain.

Domain Name: **StudioB**

Admin Password: •••••

Retype Admin Password: •••••

User Password: ••••

Retype User Password: ••••

□ Show Text

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, under **Support > Reference Articles > Factory Defaulting Ethernet Devices** for detailed instructions.

Once they reappear in Pathscape as 🔒 **Unsecured**, add them 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 or later)**, you will not be able to configure them. **You must use Pathscape 4 or later**. As a reminder, the device label will appear in the earlier versions of Pathscape as "**Use latest Pathscape PC software to secure**". Other properties will be shown and are correct, but any attempts to change them will fail.

INTRODUCING PATHWAY ssACN (Secure sACN)

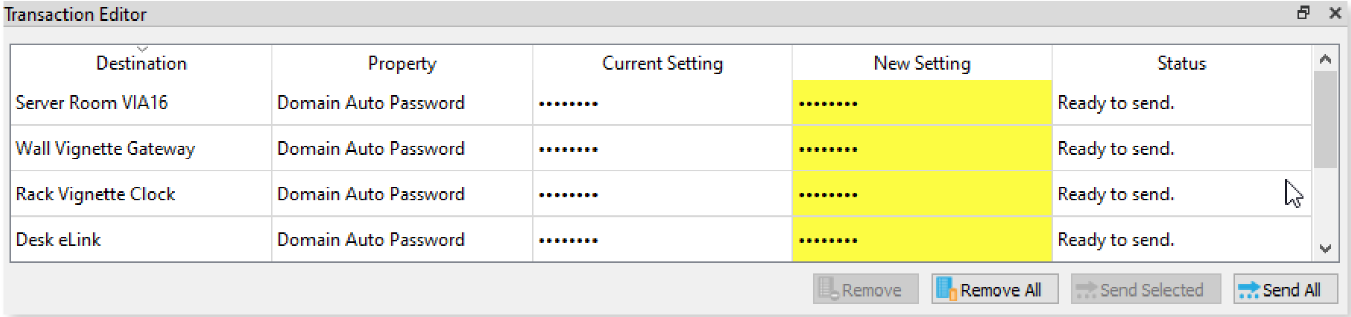
Pathway ssACN (Secure streaming ACN) is a new protocol developed by Pathway using much of ANSI E1.31, but adds a layer of authentication. This feature requires **device firmware version 6.0 or later**.

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.



Transaction Editor

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

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

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

CUSTOM ssACN PASSWORD

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

This is useful in a few situations:

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

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

USING PATHWAY ssACN WITH VIA

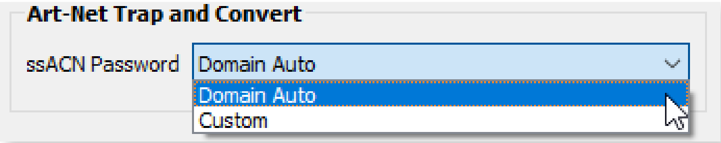
In general, VIA switches do not perform any protocol conversion on data traffic, except with the feature **Art-Net Trap and Convert.**

When **Art-Net Trap and Convert** is enabled on a Port, Art-Net data packets with broadcast address destinations are trapped and converted to E1.31 sACN or Pathway ssACN multicast packets, as the packets enter the Port of the switch.

Because VIA switches can now trap Art-Net and Convert it to Pathway ssACN, there are new properties to configure for this functionality.

In the VIA **base device** properties, there is the **Art-Net Trap and Convert** section**.**

In the **ssACN Password** drop-down menu, specify whether the switch should use the generated **Domain Auto** password (default) or a **Custom ssACN Password**.

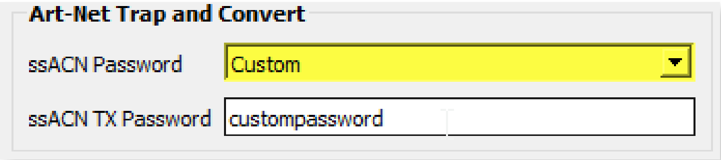


Art-Net Trap and Convert

ssACN Password: Domain Auto

NOTE: This applies only if you choose to convert Art-Net to Pathway ssACN. If you choose to convert Art-Net to standard E1.31 sACN, this setting does not apply.

If you select **Custom**, enter the Custom Pathway ssACN password in the **ssACN TX Password** field.

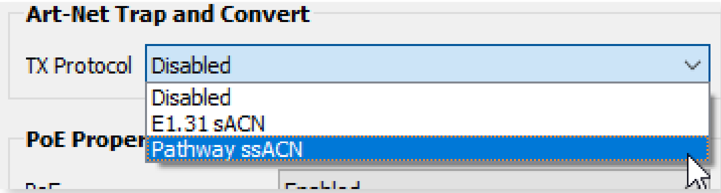


Art-Net Trap and Convert

ssACN Password: Custom

ssACN TX Password: custompassword

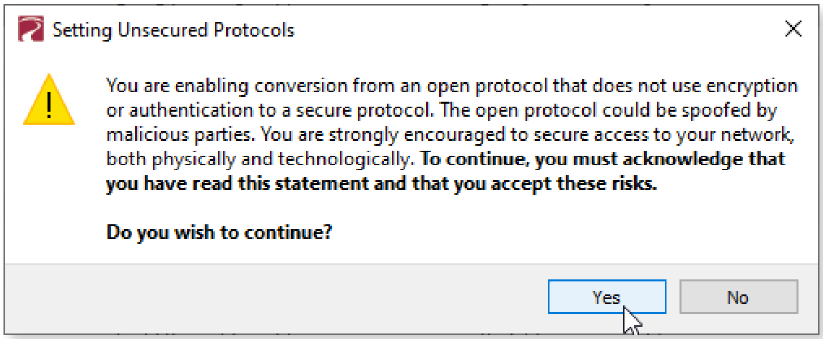
On the relevant VIA switch Ports, under the **Art-Net Trap and Convert** section, select the **TX Protocol** to convert trapped Art-Net packets to for that Port. Options are standard **E1.31 sACN** or **Pathway ssACN**. You may also choose to **disable** the function.



Art-Net Trap and Convert

TX Protocol: Disabled

When selecting Pathway ssACN as a TX Protocol, a warning message appears informing you of the risks associated with using an unsecured protocol (Art-Net). While Pathway ssACN itself is secure, the source Art-Net protocol is not. To continue, click the “Yes” button.



Setting Unsecured Protocols

You are enabling conversion from an open protocol that does not use encryption or authentication to a secure protocol. The open protocol could be 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 that you accept these risks.**

Do you wish to continue?

NOTE that the individual Port property determines what type of conversion is performed (None/Disabled, E1.31 sACN or Pathway ssACN), and the base device property determines the Pathway ssACN Password type. You may choose to convert to E1.31 sACN on some ports, Pathway ssACN on others, and disable the function on others, or any combination.

See later in this manual for more detail on Art-Net Trap & Convert.

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 can accept any number of different custom passwords.

See the **Pathscape manual** section on **Pathway ssACN** for more detail about setting and managing Pathway ssACN passwords across your network.

SOFTWARE (PATHSCAPE) CONFIGURATION

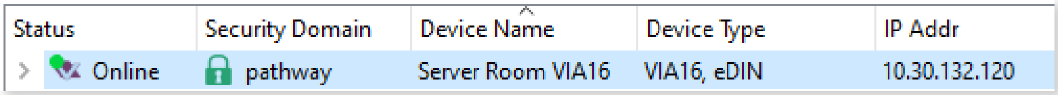
Configuration must be done using **Pathscape**. For in-depth information on using Pathscape, see the Pathscape manual. Pathscape is available for macOS and Windows from the Software section of our website: https://www.pathwayconnect.com.

NETWORK SETUP

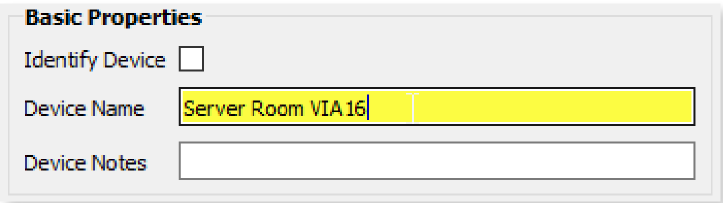
PLEASE NOTE: Before any configuration and network setup can be done, including setting the IP, the VIA switch(es) must be added to a Security Domain. If the device is not added to a Security domain, it will not be possible to configure any properties.

From the factory, the switch 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 VIA's name in the device list will be shown as its IP address. Give it a useful name before continuing.



Status	Security Domain	Device Name	Device Type	IP Addr
Online	pathway	Server Room VIA16	VIA16, eDIN	10.30.132.120



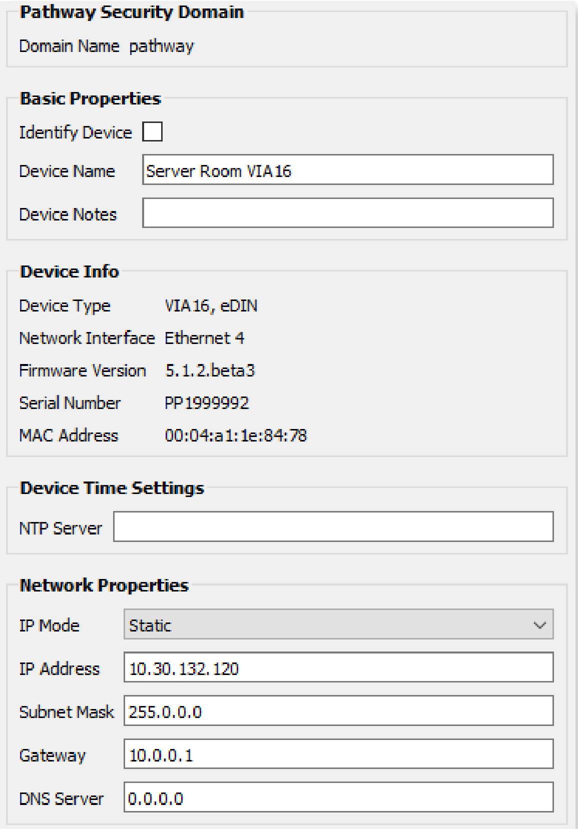
Basic Properties

Identify Device □

Device Name: Server Room VIA16

Device Notes:

DEVICE PROPERTIES



Pathway Security Domain

Domain Name pathway

Basic Properties

Identify Device □

Device Name: Server Room VIA16

Device Notes:

Device Info

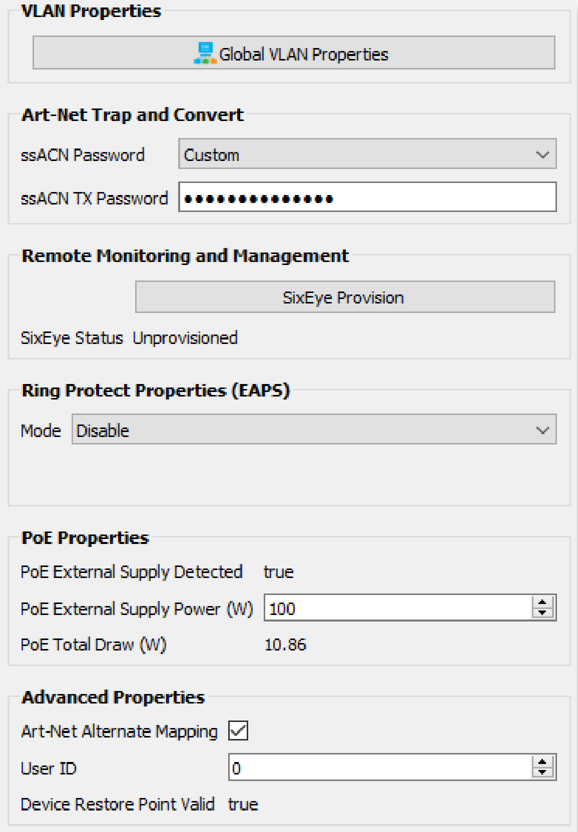
Device Type	VIA16, eDIN
Network Interface	Ethernet 4
Firmware Version	5.1.2.beta3
Serial Number	PP1999992
MAC Address	00:04:a1:1e:84:78

Device Time Settings

NTP Server:

Network Properties

IP Mode	Static
IP Address	10.30.132.120
Subnet Mask	255.0.0.0
Gateway	10.0.0.1
DNS Server	0.0.0.0



VLAN Properties

Art-Net Trap and Convert

ssACN Password: Custom

ssACN TX Password: ••••••••••••••

Remote Monitoring and Management

SixEye Status Unprovisioned

Ring Protect Properties (EAPS)

Mode: Disable

PoE Properties

PoE External Supply Detected	true
PoE External Supply Power (W)	100
PoE Total Draw (W)	10.86

Advanced Properties

Art-Net Alternate Mapping ☑

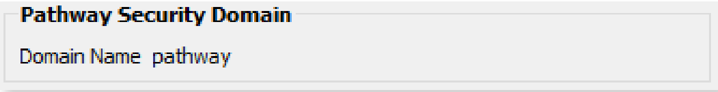
User ID: 0

Device Restore Point Valid true

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 (greyed out and uneditable), make sure you are logged into the correct Security Domain.

PATHWAY SECURITY DOMAIN



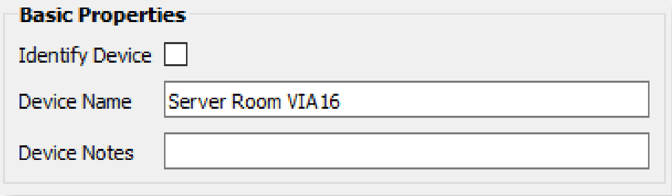
Pathway Security Domain

Domain Name pathway

DOMAIN NAME

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

BASIC PROPERTIES



Basic Properties

Identify Device □

Device Name: Server Room VIA16

Device Notes:

IDENTIFY DEVICE

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

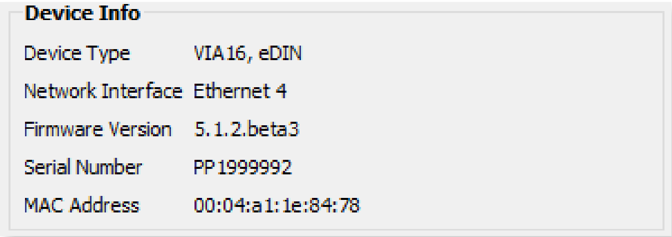
DEVICE NAME

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

DEVICE NOTES

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

DEVICE INFO



Device Info

Device Type	VIA16, eDIN
Network Interface	Ethernet 4
Firmware Version	5.1.2.beta3
Serial Number	PP1999992
MAC Address	00:04:a1:1e:84:78

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.

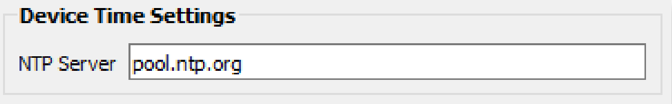
SERIAL NUMBER

Factory-set unique identifier. Read-only.

MAC ADDRESS

Factory-set hardware address. Read-only.

DEVICE TIME SETTINGS



Device Time Settings

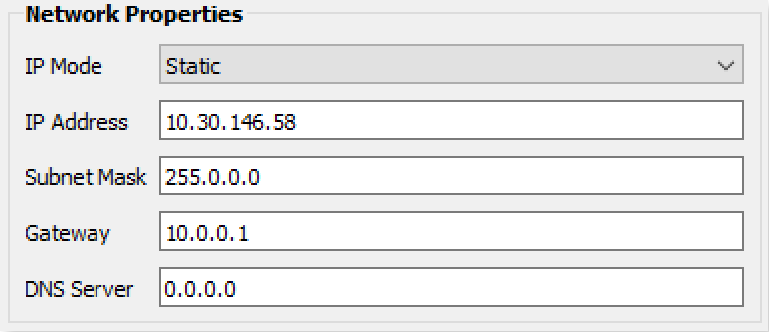
NTP Server: pool.ntp.org

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 IP Gateway are set so the device knows how to get to the Internet to find a time server.

NETWORK PROPERTIES



Network Properties

IP Mode: Static

IP Address: 10.30.146.58

Subnet Mask: 255.0.0.0

Gateway: 10.0.0.1

DNS Server: 0.0.0.0

IP ADDRESS

Internet Protocol address (IPv4) of the Gateway.

SUBNET MASK

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

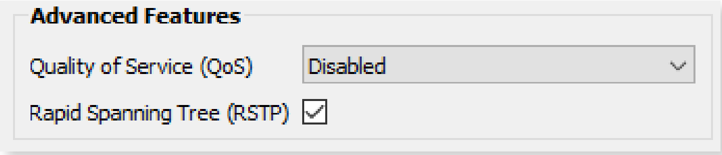
GATEWAY

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

DNS Server

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

ADVANCED FEATURES

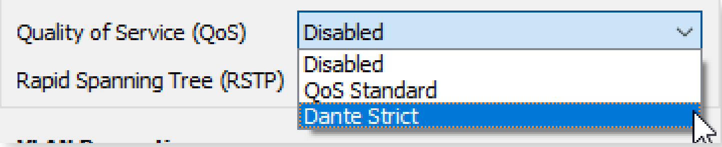


Advanced Features

Quality of Service (QoS): Disabled

Rapid Spanning Tree (RSTP) ☑

QUALITY OF SERVICE (QoS)



Quality of Service (QoS): Disabled

Rapid Spanning Tree (RSTP)

Quality of Service determines the relative priority of different data packets, which in turn determines which packets should receive preferential routing from a VIA switch. QoS is often used for the distribution of video and audio signals, including the Dante® audio standard, to meet the signal's required timing constraints.

Disabled (default): Disables QoS-based routing. All traffic is treated equally.

Standard: Traffic priority is observed using a weighted algorithm to ensure timely delivery of high priority traffic and eventual delivery of lower priority packets.

Dante Strict: Traffic priority is strictly observed, using Dante-specified weighting. Lower priority traffic may be dropped or ignored to ensure delivery of Dante's high priority packets.

NOTE: remember that giving all data high priority is the same as treating all traffic equally.

For more information, please refer to **Appendix 5: Quality of Service (QoS)**.

RAPID SPANNING TREE (RSTP)

Click the checkbox to **Enable** / **Disable** (default) Rapid Spaning Tree Protocol (RSTP)

Rapid Spanning Tree Protocol automatically detects Ethernet loops (two Cat5 cables between the same two switches where the ports are on the same VLAN). Without RSTP on, networks with loops will have very poor performance.

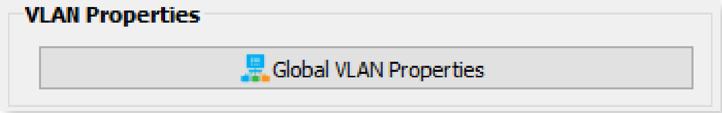
RSTP should be enabled on all switches on the network and not be used in conjunction with EAPS Ring Protection.

The interaction between RSTP and the Ring Protect system may cause long network re-configuration times when the ring topology is changed. For this reason, it is recommended that RSTP be used during setup and then disabled after verifying there are no loops present.

Warning: Rapid Spanning Tree must be enabled on all switches to detect loops correctly. Network loops created through un-managed switches may not be detected correctly. Pathway's implementation of Rapid Spanning Tree Protocol should be inter-operable with other switch manufacturer's implementations.

For more information, please refer to **Appendix 4: EAPS & RSTP - Ring Protection**.

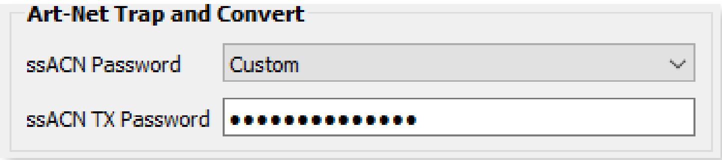
VLAN PROPERTIES



To enable/disable VLANs, click the **Global VLAN Properties** Button.

For more information on setting VLAN Properties, see the **VLAN Configuration** section later in this manual.

Art-Net TRAP AND CONVERT



ssACN Password: Custom

ssACN TX Password: ••••••••••••••

When enabled, Art-Net data packets with broadcast address destinations are trapped and converted to E1.31 sACN or Pathway ssACN multicast packets, as the packets enter the port of the switch.

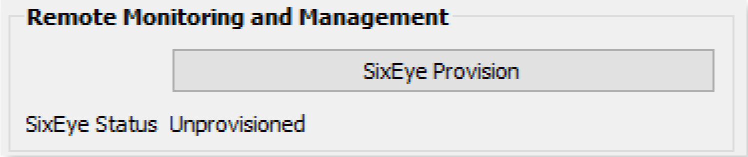
ssACN PASSWORD.

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. Enter a custom TX password here.

See the **Introducing Pathway ssACN** section earlier in this manual for more details.

REMOTE MONITORING AND MANAGEMENT



SixEye Status Unprovisioned

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.

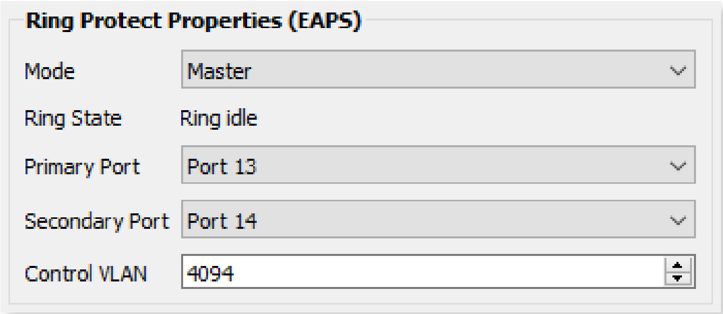
SixEye Init Error. The device could not initiate a connection with SixEye.

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

Connected. The device is connected to SixEye.

RING PROTECT PROPERTIES (EAPS)

Allows VIA switches to be connected in a physical wiring ring using EAPS (Ethernet Automatic Protection Switching. See **Appendix 4: EAPS & RSTP - Ring Protection** for details).



Ring Protect Properties (EAPS)

Mode: Master

Ring State: Ring idle

Primary Port: Port 13

Secondary Port: Port 14

Control VLAN: 4094

MODE

Set the function for Ring Protect Mode.

Disable (default): Ring Protect is disabled. **When set to Disabled, the remaining Properties below are hidden**.

Transit: Sets the selected switch to act as a Transit switch.

Master: Sets the selected switch to act as the Master switch.

RING STATE

Shows the current state of the Ring. Values are:

Ring Idle. The ring is not currently doing anything; seen after enabling Ring Protect but before any attempt to initialize the ring has happened.

Ring Complete. The ring is initialized and working. The Master switch is monitoring the health of the ring.

Ring Failed. The ring integrity is broken.

Ring Initializing. The ring is currently initializing.

PRIMARY PORT

Select the port to be used as the Ring Primary Port. The Ring Primary Port must be one of the **last 4 ports** on the switch and must be different from the Secondary Port.

SECONDARY PORT

Select the port to be used as the Ring Secondary Port. The Ring Secondary Port must be one of the **last 4 ports** on the switch and must be different from the Primary Port.

CONTROL VLAN

Specifies dedicated Ring Protect VLAN. Valid range is 1 – 4095. Use of the default (4094) is strongly recommended. The Ring Protect VLAN **must to be outside of defined VLAN range**.

NOTES ON VLAN SETUP

During the set up and configuration of the Ring Protection feature, communication between devices may be erratic or broken. We strongly recommend that all switches be configured with the appropriate Ring Protection settings PRIOR to be connected together. We also strongly recommend that all switches be disconnected from one another PRIOR to disabling the ring feature.

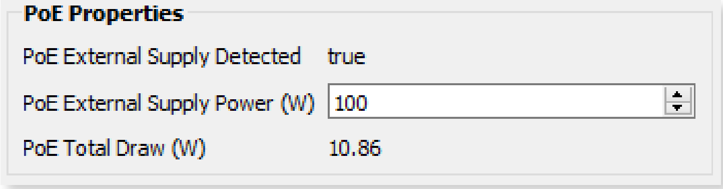
Prior to set up, determine which switch will be the master. Generally, the least busy switch with the most stable power source is the best choice. All other switches must be configured as transit switches.

All switches must have both a primary and a secondary ring port set. These ports will be automatically configured as Tagged (uplink) ports, meaning all traffic on all VLANs will be passed through the ports.

If changes are made to the ring configuration while the ring is active, it may be necessary to reboot all switches for the changes to take effect.

For additional details, see **Appendix 4: EAPS & RSTP - Ring Protection**.

PoE PROPERTIES



PoE Properties

PoE External Supply Detected true

PoE External Supply Power (W) 100

PoE Total Draw (W) 10.86

PoE EXTERNAL SUPPLY DETECTED

Will show **true** if the VIA Switch detects an external PoE supply, **false** if it does not (if applicable). Read-only.

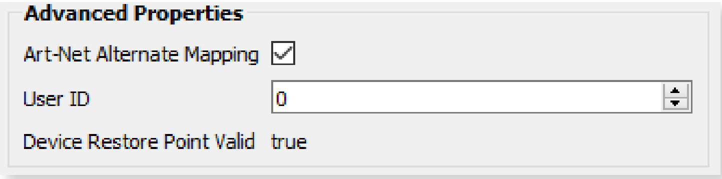
PoE EXTERNAL SUPPLY POWER (W)

When attaching an external PoE supply, the power rating in Watts **must be entered here** for the Switches' PoE to function properly.

PoE TOTAL DRAW (W)

Will display the total cumulative PoE power draw across all PoE-enabled ports, in Watts. Read-only.

ADVANCED PROPERTIES



Advanced Properties

Art-Net Alternate Mapping ☑

User ID 0

Device Restore Point Valid true

ART-NET ALTERNATE MAPPING

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

This feature is used in conjunction with the "**Art-Net Trap and Convert**" feature. **It is a device parent-level property;** it is enabled across the entire device. The Art-Net Trap and Convert property can be enabled on a port-by-port basis.

The Art-Net protocol uses two hexadecimal numbers, a 'subnet' and a 'universe', to define its DMX universe numbering. Numbering is usually shown as # - # and the valid range is from 0 - 0 (zero-zero) to F- F.

However, most other common protocols, including sACN, do not have a universe 'zero'. The issue is compounded because some early Art-Net implementations are shown in a straight decimal representation (1, 2, 3, 4…) without any indication if "1" corresponds to Art-Net universe 0-0 or to 0-1. **Art-Net controllers are strongly urged not to transmit on 0-0**.

By default, Art-Net Universe 0-0 is ignored by the VIA and the packets discarded. When Art-Net Alternate Mapping is enabled, VIA switches will map Art-Net Universe 0-0 to Pathscape Universe 1. When Alternate Art-Net Mapping is disabled, Art-Net Universe 0-0 will be ignored by the VIA and Art-Net Universe 0-1 will be routed as Pathscape Universe 1.

USER ID

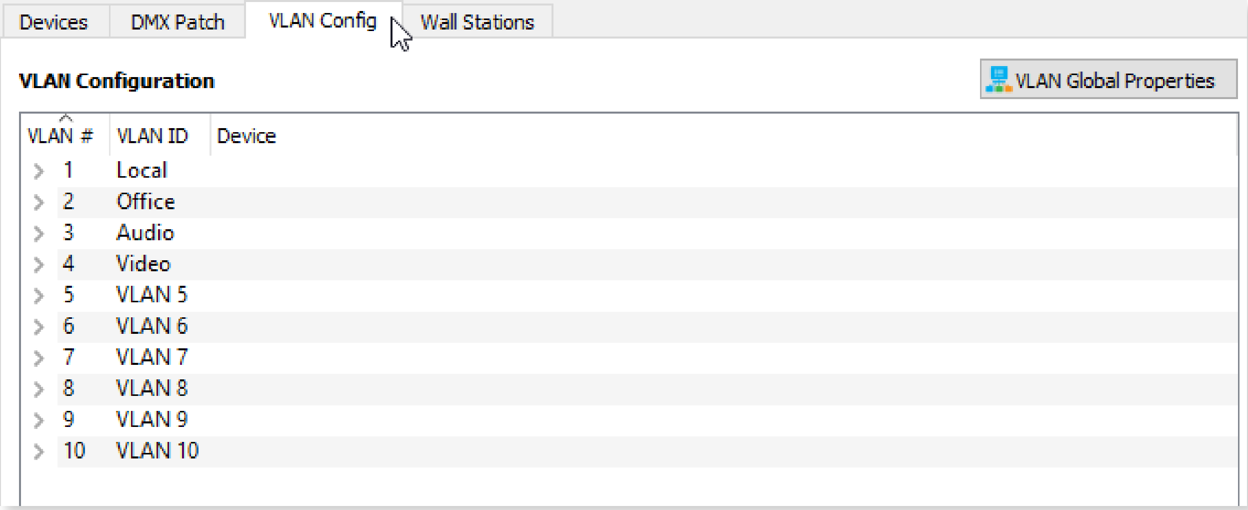
Custom numeric identification for external databases.

DEVICE RESTORE POINT VALID

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

VLAN CONFIG

Use the **VLAN Config** tab to configure network VLANs. A **VLAN** (**V**irtual **L**ocal **A**rea **N**etwork) is a group of ports on the switch (or switches) that are configured to pass traffic to one another, but not to ports on any other VLAN. When VLANs are established, ports that connect switches to switches must be "tagged" to pass all VLAN traffic. See **Appendix 3: VLANs** for further details on how to use VLANs.

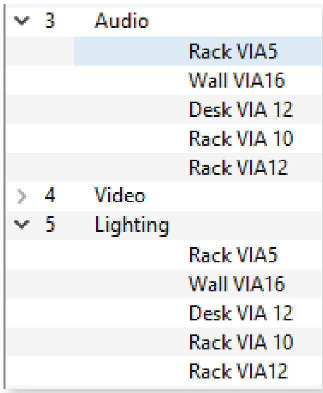


VLAN Configuration

VLAN #	VLAN ID	Device
1	Local	
2	Office	
3	Audio	
4	Video	
5	VLAN 5	
6	VLAN 6	
7	VLAN 7	
8	VLAN 8	
9	VLAN 9	
10	VLAN 10	

In the VLAN Configuration window, there are three columns: **VLAN #**, **VLAN ID**, and **Device**. By default, the VLAN ID will likely not have unique names as seen in the example above, but simply labeled "VLAN 1", "VLAN 2", etc.

Click on the arrow next to each VLAN to see the Devices (PWVIA Switches) available for configuration.



3	Audio	
		Rack VIA5
		Wall VIA16
		Desk VIA 12
		Rack VIA 10
		Rack VIA12
4	Video	
5	Lighting	
		Rack VIA5
		Wall VIA16
		Desk VIA 12
		Rack VIA 10
		Rack VIA12

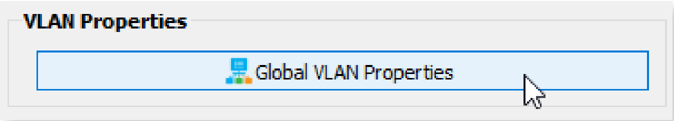
Note that every VIA Switch on the network will show up under every listed VLAN. VLAN ranges are configured Globally; it is not possible to assign a Switch to only one VLAN in this window. At the Subdevice/Port level, VLANs may be assigned as needed.

VLAN Properties such as **IP Address**, **DHCP** and **IGMP** settings are configured per VLAN per Switch. For example, to configure **VLAN 3** (Audio VLAN) as illustrated above, expand **VLAN 3** and click on the Switch device, and edit its Properties in the Properties pane. To edit **VLAN 5** on the same switch, expand **VLAN 5** and click on the Switch to edit **VLAN 5** on that device.

VLAN Properties are described below.

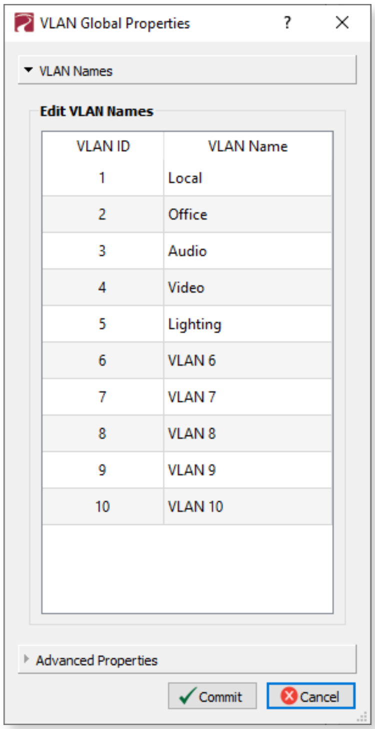
VLAN GLOBAL PROPERTIES

In order to use VLANs, **VLAN Support** must be enabled in **VLAN Global Properties**, which is accessed by clicking the VLAN Global Properties button in the top-right corner of the window. You can also click this button in the **VLAN Properties** section of the base device properties.



VLAN Properties

Global VLAN Properties



VLAN Global Properties ? ×

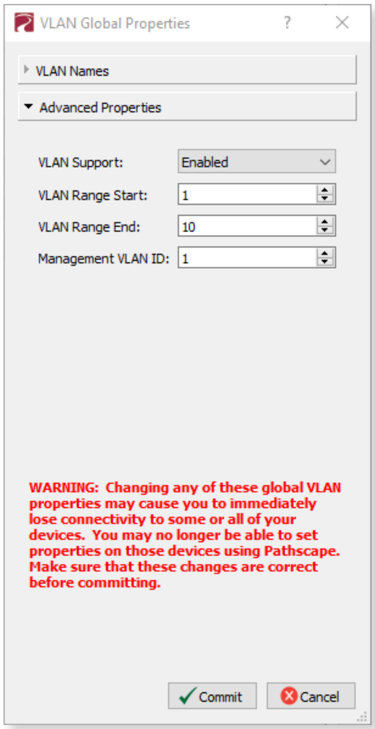
▾ VLAN Names

Edit VLAN Names

VLAN ID	VLAN Name
1	Local
2	Office
3	Audio
4	Video
5	Lighting
6	VLAN 6
7	VLAN 7
8	VLAN 8
9	VLAN 9
10	VLAN 10

▸ Advanced Properties

✓ Commit ⊗ Cancel



VLAN Global Properties ? ×

▸ VLAN Names

▾ Advanced Properties

VLAN Support: Enabled

VLAN Range Start: 1

VLAN Range End: 10

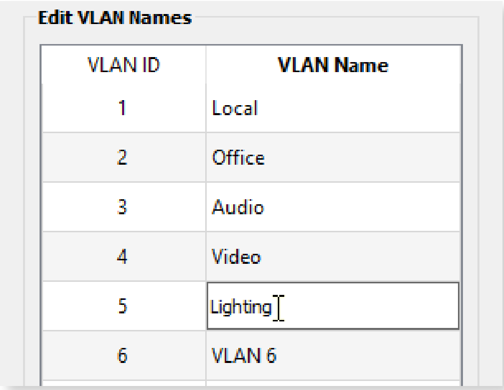
Management VLAN ID: 1

WARNING: Changing any of these global VLAN properties may cause you to immediately lose connectivity to some or all of your devices. You may no longer be able to set properties on those devices using Pathscape. Make sure that these changes are correct before committing.

✓ Commit ⊗ Cancel

There are two sections to the VLAN Global Properties window, the **VLAN Names** panel, and the **Advanced Properties** panel.

In the **VLAN Names** panel you may edit the names of any of the available VLANs by double-clicking on the VLAN Name, editing it and then clicking the ✓ Commit button.



Edit VLAN Names

VLAN ID	VLAN Name
1	Local
2	Office
3	Audio
4	Video
5	Lighting
6	VLAN 6

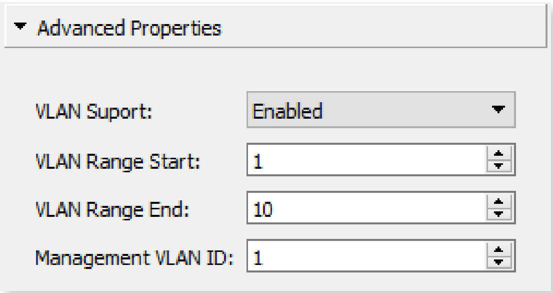
You will then see several transactions populate in the transaction editor, which will be automatically sent. To discard changes, click the ⊗ Cancel button.

The **Advanced Properties** panel will allow for global configuration of VLAN Ranges, Management VLAN, and VLAN Support on and off.

⚠ WARNING ⚠

Changing any of these global VLAN properties may cause you to immediately lose connectivity to same or all of your devices. You may no longer be able to set properties on those devices using Pathscape. Make sure that these changes are correct before committing.

See Appendix 3: VLANs for futher details on how to use VLANs.



▾ Advanced Properties

VLAN Suport: Enabled

VLAN Range Start: 1

VLAN Range End: 10

Management VLAN ID: 1

The **VLAN Support** drop-down allows for enabling or disabling of VLANs.

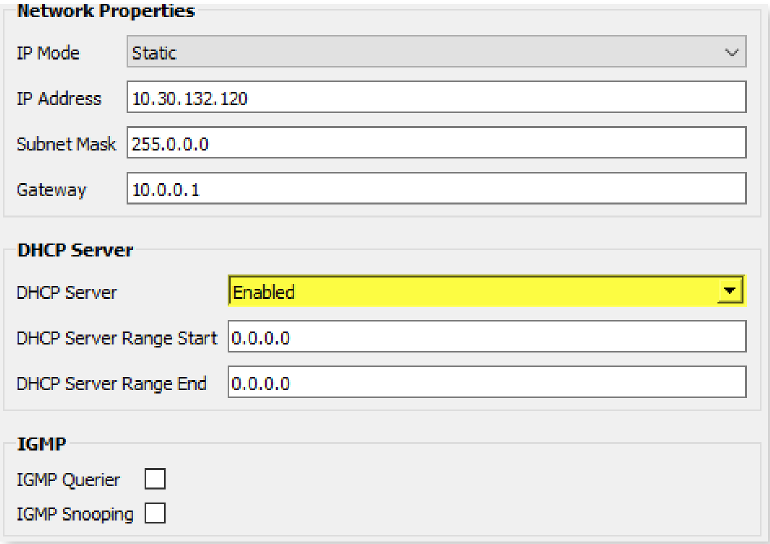
VLAN Range Start and **VLAN Range End** will determine the range of VLAN IDs available to use. Default is 1 and 10, respectively. To edit the start and end ID values, either type into the text fields or click on the up and down arrows to modify the value. To make the desired changes, click the ✓ Commit button. You will then see several transactions populate in the transaction editor, which will be automatically sent. To discard changes, click the ⊗ Cancel button.

Management VLAN ID sets which VLAN is used by the switch management processor(s). Default is 1. **It is strongly recommended that the Management VLAN ID be set to the same value as the VLAN Range Start value. Care must be taken that the Management VLAN is used by at least one Normal/Untagged port on the switch, or the ability to configure the switch may be lost.**

See Appendix 3: VLANs for futher details on how to use VLANs.

VLAN PROPERTIES/SERVICES

VLANs must be enabled prior to configuring these services. You will find the VLAN Enable/Disable Property in the **VLAN Global Properties Window** in the VLAN Config window or under the **Settings Menu**.



Network Properties

IP Mode: Static

IP Address: 10.30.132.120

Subnet Mask: 255.0.0.0

Gateway: 10.0.0.1

DHCP Server

DHCP Server: Enabled

DHCP Server Range Start: 0.0.0.0

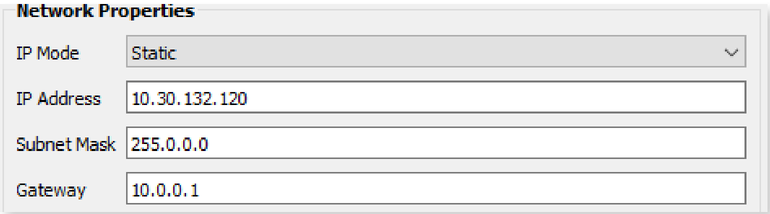
DHCP Server Range End: 0.0.0.0

IGMP

IGMP Querier □

IGMP Snooping □

NETWORK PROPERTIES



Network Properties

IP Mode: Static

IP Address: 10.30.132.120

Subnet Mask: 255.0.0.0

Gateway: 10.0.0.1

IP MODE

Disabled: No IP assigned to this VLAN by this VIA

Static: IP settings manually set by user (default for VLAN ID#1 / management VLAN). You must set a Static IP address if you want to enable DHCP and/or IGMP on this VLAN.

Dynamic: IP settings obtained from DHCP server.

IP ADDRESS

User-configured Internet Protocol address (IPv4) for this switch on the selected VLAN.

SUBNET MASK

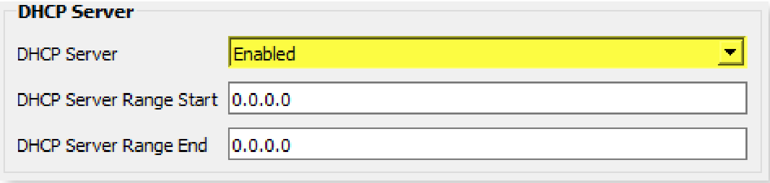
User-configured subnet mask applied to VLAN.

GATEWAY

Network traffic on this VLAN requesting addresses outside of the assigned subnet will be routed through this IP address.

DHCP PROPERTIES

DHCP SERVER



DHCP Server

DHCP Server: Enabled

DHCP Server Range Start: 0.0.0.0

DHCP Server Range End: 0.0.0.0

Dynamic Host Configuration Protocol (DHCP).

Disabled (default).

Enabled: Only one switch on a given VLAN may have an active DHCP service, and that VLAN must have a static IP itself. One switch with multiple VLANs may have multiple DHCP servers.

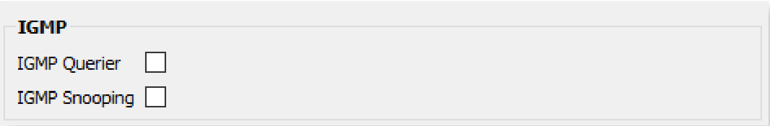
DHCP SERVER RANGE START

Sets start IP address in the DHCP pool. Pool must begin at an address higher than the IP address of the server.

DHCP SERVER RANGE END

Sets last available IP address in the DHCP pool. Cannot exceed the last valid IP value in the IP/Subnet Mask range.

IGMP



IGMP

IGMP Querier □

IGMP Snooping □

Intergroup Management Protocol (**IGMP**) allows for packet filtering and forwarding by the switch based on multicast groups. Networks using sACN can take full advantage of IGMP by reducing the traffic on the link to the gateway to just the xDMX Universes the gateway is configured to listen to.

IGMP QUERIER

Disabled (default).

Enabled: Allows switch to query and construct a forwarding-table based on end device subscriptions to multicast group addresses. (i.e., the Querier can tell that a 2-port DMX512 gateway is interested in Univ 8 and Univ 37, if so patched, and will route those sACN Universes, and only those, on the link on which the gateway is connected.) One querier is required be active on a given VLAN using IGMP routing. However, for reliability reasons, it is highly recommended to have two or more.

IGMP SNOOPING

Disabled (default)

Enabled: Allows the switch to forward multicast data packets according to IGMP forwarding-tables build by the Querier. All switches on a VLAN using IGMP should have snooping enabled, including the switches acting as an IGMP Querier.

NOTES ON IGMP

The IGMP Querier establishes a table of active multicast groups by querying connected devices about which multicast groups each device wishes to join. For example, a gateway will request the multicast groups associated with the sACN universes that the gateway is patched to.

Each switch operating an IGMP Querier on a VLAN must have valid IP settings on that VLAN. The IP settings may be static or dynamically established using the DHCP.

IMPORTANT: Two IGMP queriers should be active on each VLAN using multicast filtering. If no querier is active, the groupings table will fail after approximately five minutes and filtering will only work erratically or will fail altogether. IGMP should not be enabled on more than four VLANs per switch.

The IGMP Snooper allows the switch to more efficiently route multicast traffic by applying the multicast groupings as a filter. Multicast traffic is only directed to only those ports, i.e. end devices, that have requested to receive that traffic.

Watch the following video on Pathway's YouTube channel for a detailed explanation of IGMP Snooping:

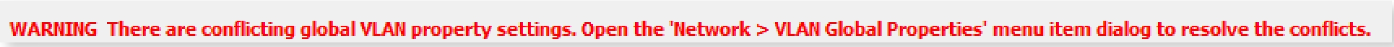
https://www.youtube.com/watch?v=0MVE22JClt4

And the following video for a real-world example.

https://www.youtube.com/watch?v=CdXl_Q7KZC0

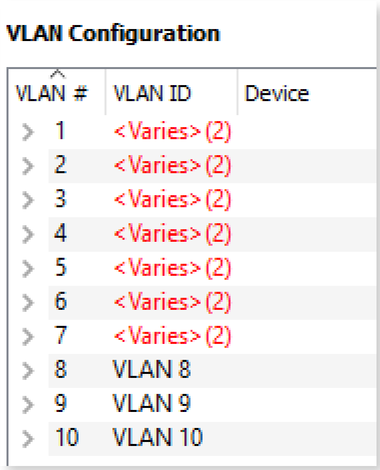
RESOLVING VLAN CONFLICTS

If you have set up your VLANs as described above, and you later add another VIA switch to your network that has different VLAN settings, you will likely see the following message in red at the bottom of the Pathscape window:



WARNING There are conflicting global VLAN property settings. Open the 'Network > VLAN Global Properties' menu item dialog to resolve the conflicts.

Go to the **VLAN Config** tab and you will see something like this:



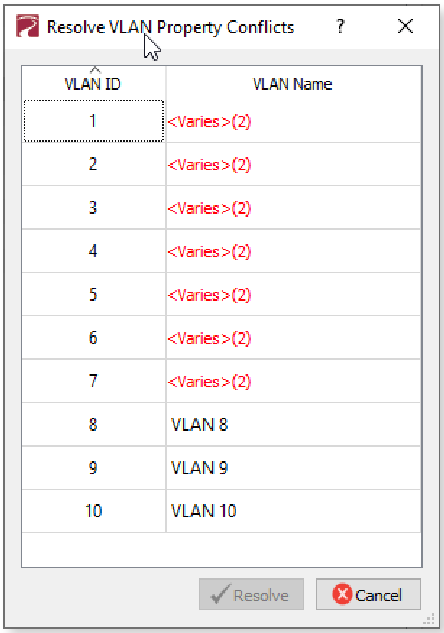
VLAN Configuration

VLAN #	VLAN ID	Device
1	<Varies> (2)	
2	<Varies> (2)	
3	<Varies> (2)	
4	<Varies> (2)	
5	<Varies> (2)	
6	<Varies> (2)	
7	<Varies> (2)	
8	VLAN 8	
9	VLAN 9	
10	VLAN 10	

Because the VLAN properties are stored on each physical VIA switch, when a new switch comes online with different property values, Pathscape doesn't know which one(s) to use. For each VLAN ID that has multiple values associated with it, Pathscape will instead list the ID as "**<Varies> (X)**" with X being the number of different values found across all switches.

As described above, Pathscape requires VLAN settings to be Global across the entire network, so only one set of VLAN properties (including ID, VLAN Enable/Disable, VLAN Range, and Management VLAN) may be used.

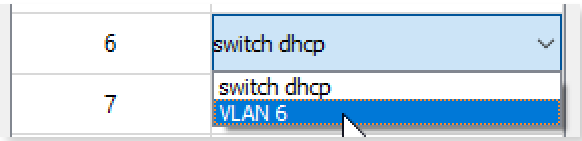
You will have to resolve the conflicts before you can continue. Click the VLAN Global Properties button, and the **Resolve VLAN Property Conflicts** window will open.



Resolve VLAN Property Conflicts

VLAN ID	VLAN Name
1	<Varies>(2)
2	<Varies>(2)
3	<Varies>(2)
4	<Varies>(2)
5	<Varies>(2)
6	<Varies>(2)
7	<Varies>(2)
8	VLAN 8
9	VLAN 9
10	VLAN 10

For each VLAN ID with conflicting properties, you will need to double-click on each instance of "**<Varies> (X)**" and then pick the correct VLAN ID from the drop-down menu.



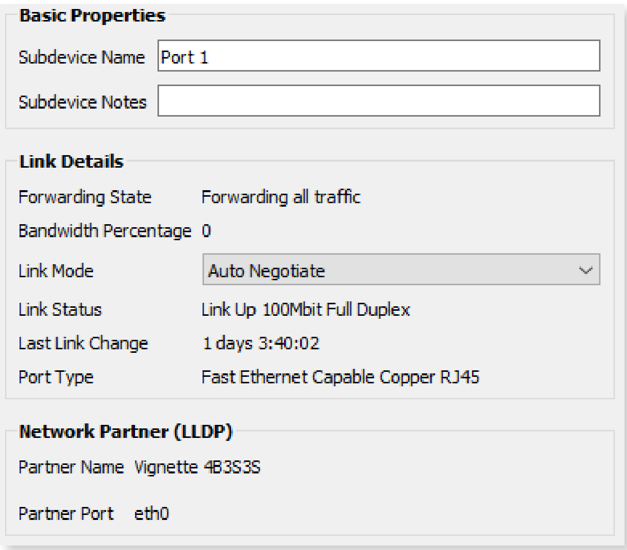
Pathscape will then use the settings associated with those VLAN IDs chosen to clear the found conflicts

PORT PROPERTIES AND CONFIGURATION

VIA Switch subdevices are Ethernet Ports, either copper RJ45 Ports or SFP/fiber ports. The color of the Port icon reflects its Link Status and Speed.

Icon	Status
Grey RJ45	Copper RJ4: Link Down (no downstream device connected)
Blue RJ45	Copper RJ45: 1 Gigabit (PWVIA DIN P8 Only)
Green RJ45	Copper RJ45: 100 Megabit, full or half duplex
Orange RJ45	Copper RJ45: 10 Megabit full or half duplex
Grey Fiber	SFP/Fiber: Link Down (no downstream device connected)
Blue Fiber	SFP/Fiber: 1Gigabit
Purple Fiber	SFP/Fiber: 10Gigabit (PWVIA DIN P8 Only)

Not all properties are supported by all VIA models. Only the properties supported by the selected switch's port will be shown in the Properties Pane.



Basic Properties

Subdevice Name: Port 1

Subdevice Notes:

Link Details

Forwarding State: Forwarding all traffic

Bandwidth Percentage: 0

Link Mode: Auto Negotiate

Link Status: Link Up 100Mbit Full Duplex

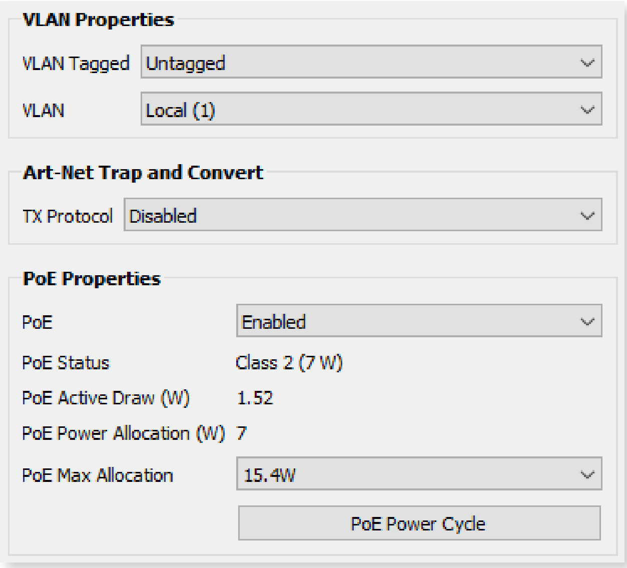
Last Link Change: 1 days 3:40:02

Port Type: Fast Ethernet Capable Copper RJ45

Network Partner (LLDP)

Partner Name: Vignette 4B3S3S

Partner Port: eth0



VLAN Properties

VLAN Tagged: Untagged

VLAN: Local (1)

Art-Net Trap and Convert

TX Protocol: Disabled

PoE Properties

PoE: Enabled

PoE Status: Class 2 (7 W)

PoE Active Draw (W): 1.52

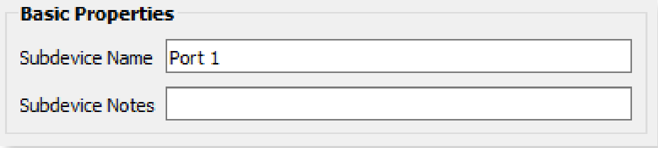
PoE Power Allocation (W): 7

PoE Max Allocation: 15.4W

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

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

BASIC PROPERTIES



Basic Properties

Subdevice Name	Port 1
Subdevice Notes	

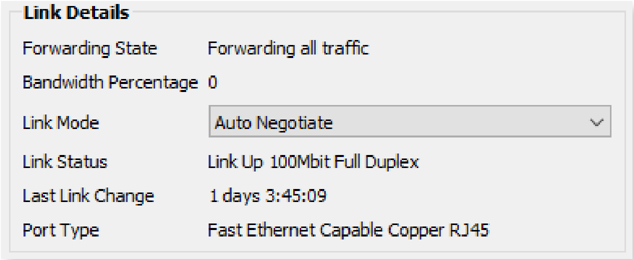
SUBDEVICE NAME

A user-configured, soft label for the subdevice/Port. Shown in the Device view and on the front panel display of the Switch (if equipped).

SUBDEVICE NOTES

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

LINK DETAILS



Link Details

Forwarding State	Forwarding all traffic
Bandwidth Percentage	0
Link Mode	Auto Negotiate
Link Status	Link Up 100Mbit Full Duplex
Last Link Change	1 days 3:45:09
Port Type	Fast Ethernet Capable Copper RJ45

FORWARDING STATE

Status of RSTP and EAPS. Read-only.

Forwarding all Traffic: Normal state.

Blocked by RSTP: Loop detected and port blocked to stop feedback.

Blocked by EAPS: Ring using primary port.

BANDWIDTH PERCENTAGE

Reports a number between 0 and 100 based on Link Mode showing the amount of traffic going through the port. Readings are updated every few seconds. Read-only.

LINK MODE

Configures the Link Mode for the specified port.

Disable: Effectively turns port off.

Auto Negotiate (default): Link speed set by negotiation between switch and end device.

10Mbit Half Duplex

10Mbit Full Duplex

100Mbit Half Duplex

100Mbit Full Duplex

1Gbit Full Duplex (1Gbit Copper Ports Only - PWVIA DIN P8, SFP Ports - PWVIA DIN P16, SFP+ Ports - PWVIA DIN P8)

10Gbit Full Duplex (SFP+ Ports Only - PWVIA DIN P8)

LINK STATUS

Reports current link status and speed. Read Only.

LAST LINK CHANGE

Displays the time elapsed since the last change in the Port Link Status. Shown as **X Days, HH:MM:SS** (Hours:Minutes:Seconds). Useful for diagnostic or troubleshooting purposes to determine if a Port has gone down unexpectedly, for example.

SFP MODULE TYPE

Reports the detected type of SFP (Small Form-factor Pluggable) fiber optics transceiver. Read Only. Applicable to Ports 17 and 18 on **PWVIA DIN P16 only**.

SFP+ MODULE TYPE

Reports the detected type of SFP+ (enhanced Small Form-factor Pluggable) fiber optics transceiver. Read Only. Applicable to Ports 9 and 10 on **PWVIA DIN P8 only**.

PORT TYPE

Reports Port Type. Read-only.

Gigabit Capable Fiber

10 Gigabit Capable Fiber (PWVIA DIN P8 Only)

Gigabit Capable Copper RJ45 (PWVIA DIN P8 Only)

Fast Ethernet Capable Copper RJ45

NETWORK PARTNER (LLDP)

PARTNER NAME

If the connected device supports Link Layer Discovery Protocol (LLDP), such as Vignette Wall statoin (PWWSI) devices, Pathport gateways (PWPP), and other VIA switches, the connected device's name will appear here. Read-only.

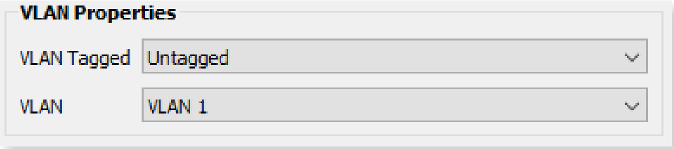
PARTNER PORT

If the connected device supports Link Layer Discovery Protocol (LLDP), this will show the Port Number on that device that this port is connected to.

If the connected device is not a switch and has only one port, this will show "Eth".

VLAN PROPERTIES

Set VLAN Properties for the selected port.



VLAN Properties

VLAN Tagged: Untagged

VLAN: VLAN 1

VLAN TAGGED

When VLANs are enabled, set port as a **Tagged/Uplink** to transmit all VLANs' data between switches. Typically tagged ports are only used to connect a switch to a switch. Although it is possible to make a PC's NIC tagged, Pathway gateways and controllers do not used tagged NICs. If you cannot communicate with a gateway or controller, check that the port your PC is using and the port the devices is on are not tagged and on the same VLAN.

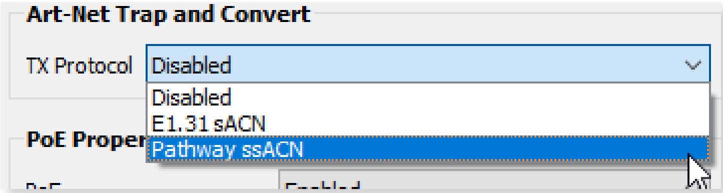
For most applications, **ports connected to end devices** should be set as **Untagged** (default).

VLAN

Sets the VLAN ID# used by the port. Only applies to untagged ports when VLANs have been enabled.

Art-Net TRAP AND CONVERT

See also **Art-Net Alternate Mapping** in the base device properties.



Art-Net Trap and Convert

TX Protocol: Disabled

TX PROTOCOL

Disabled (default).

E1.31 sACN: Any inbound Art-Net broadcast packets are converted to **E1.31 sACN** multicast data packets using the same Universe number as originally transmitted. On large systems using sACN, you should enable IGMP to reduce network traffic.

Pathway ssACN: Any inbound Art-Net broadcast packets are converted to **Pathway Secure sACN (ssACN)** multicast data packets using the same Universe number as originally transmitted. On large systems using sACN, you should enable IGMP to reduce network traffic.

NOTES ON Art-Net TRAP AND CONVERT

When enabled, Art-Net data packets with broadcast address destinations are trapped and converted to E1.31 sACN multicast packets, as the packets enter the port of the switch. The resulting sACN packets may then be filtered using the IGMP settings.

Art-Net Trap and Convert is a port-level property; it can be enabled on a port-by-port basis.

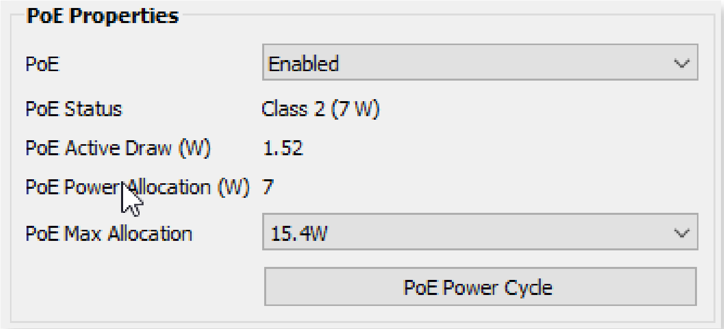
When enabled, Art-Net data packets with broadcast address destinations are trapped and converted to E1.31 sACN multicast packets, as the packets enter the port of the switch. The resulting multicast sACN packets may then be filtered using the IGMP settings. All other Art-Net broadcast packets, such as ArtPoll, are discarded. Depending on the amount of Art-Net data traffic, this operation could significantly improve bandwidth usage efficiency and reduce the amount of unnecessary traffic seen by end devices.

The Art-Net packet will be converted to the analogous sACN universe. Due to how Art-Net universes are numbered, there is the possibility of an off-by-one error. Change the "Art-Net Alternate Mapping" option should the universe mapping seem incorrect.

Although performance depends on DMX frame rate, conversion of no more than 48 Art-Net universes by one VIA at one time is recommended.

When this feature is disabled, Art-Net data will be routed as normal broadcast traffic to all devices on the current VLAN.

POE PROPERTIES



PoE Properties

PoE: Enabled

PoE Status: Class 2 (7 W)

PoE Active Draw (W): 1.52

PoE Power Allocation (W): 7

PoE Max Allocation: 15.4W

PoE

Enabled (default): Port will attempt to power any connected PoE-compliant device. The green PoE LED (Ports 1-12 on PWVIA DIN P16, all ports on PWVIA DIN P8) will be lit.

Disabled: PoE will not be provided to end devices. The green PoE LED will not be lit.

PoE STATUS

PoE Class as reported by end device. Read-only.

Not Detected (end device not PoE)

Class 0 (15.4W)

Class 1 (5.4W)

Class 2 (11.7W)

Class 3 (15.4W)

PoE ACTIVE DRAW (W)

Reports current PoE device draw in Watts. Read-only.

PoE POWER ALLOCATION (W)

Reports power allocation to port based on end device's reported PoE device classification. Read-only.

PoE MAX ALLOCATION

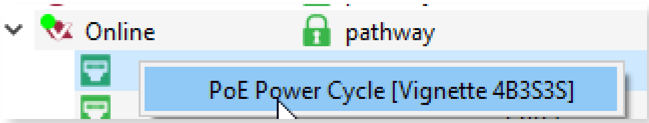
Sets power allocated to port. Allows switch to determine remaining PoE power pool available, but does not prevent end devices from requesting and utilizing power in excess of this value.

Values are **900mW, 1.8W, 2.7W, 3.6W, 4.5W, 5.4W, 6.3W, 7.2W, 8.1W, 9W, 9.9W, 10.8W, 11.7W, 12.6W, 13.5W, 14.4W and 15.4W**.

PoE POWER CYCLE

Clicking this button will disable and then re-enable PoE on the selected port, in order to power cycle the end device.

You can also right-click any VIA Port in the Device view and select PoE Power Cycle.



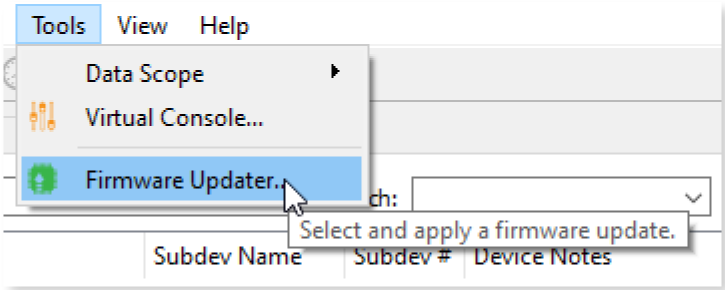
If the connected device supports LLDP, the device's name will appear so you know exactly what device you're power cycling

UPGRADING DEVICE FIRMWARE

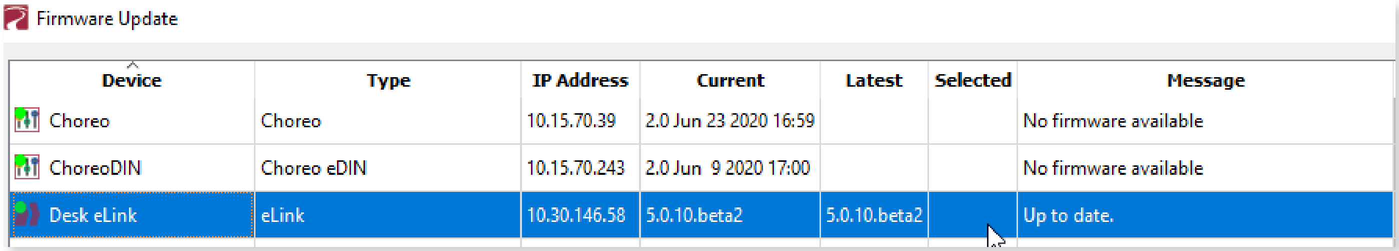
Firmware upgrades may only be done using Pathscape.

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

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



This will bring up the Firmware Update window.



Device	Type	IP Address	Current	Latest	Selected	Message
Choreo	Choreo	10.15.70.39	2.0 Jun 23 2020 16:59			No firmware available
ChoreoDIN	Choreo eDIN	10.15.70.243	2.0 Jun 9 2020 17:00			No firmware available
Desk eLink	eLink	10.30.146.58	5.0.10.beta2	5.0.10.beta2		Up to date.

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.**

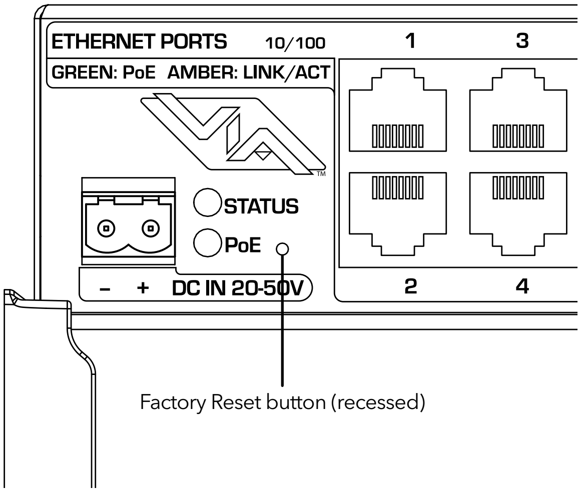
It is strongly recommended that you do not update VIA Switches and connected PoE devices at the same time. It is possible for the firmware update process to reboot the Switch before the data has finished writing to the PoE devices' memory. If the VIA Switch reboots at this point, the connected PoE devices' 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 (eg. Management VLAN accidentally set to a value outside the VLAN range), it is possible to reset the switch to factory settings.

While powered, insert the tip of a pen or paperclip into the small hole in the front panel next to the PoE LED and press and hold the reset button for 5 seconds.



The device will then reboot, having reset itself to the Factory settings. Before configuration can be restored, the unit must be secured by adding it to a Security Domain.

APPENDIX 1: SFP/SFP+ FIBER ADAPTER SELECTION

VIA switches allow the end user to provide a fiber adaptor. The adaptors are typically referred to as an SFP (Small Form Pluggable transceiver) or mini-GBIC (gigabit interface converter).

Pathway part number PWACC SFP is an SFP 850nm Ethernet Optical Transceiver that is compatible with PWVIA RM P12, PWVIA DIN P16 and PWVIA DIN P8, capable of 1Gbps. Part number PWACC SFPP is a dual-rate SFP+ 850nm Ethernet Optical Transceiver capable of 10Gbps, compatible with the PWVIA DIN P8 and PWVIA RM P12 models. These fiber links can go up to 550 m (1800 feet) without issue. In some situations, the run lengths may lead you to choose a different SFP. Follow these guidelines when choosing your SFP:

1. The form factor must be stated as SFP or SFP+ (not XENpack or others).
2. The fiber connector is LC Duplex.
3. The SFP must support Optical Gigabit Ethernet (typically referred to as 1000BASE-SX, 1000BASE-LX, 10GBase-SR or 10GBase-LR)
4. The SFP must match the type of fiber installed, either Single Mode or Multi-Mode.
5. The SFP must support the distance required, which in turn determines the optical wavelength. 850nm is typically used for runs up to 550m, while 1310nm is typically used for runs up to 10km.

We strongly recommend each end of the connection use an identical SFP.

When the SFP module is inserted in the switch, the Link/Status LED will light up **green**. If an incompatible module is detected, the Link/Status LED will light up **red**. In Pathscape the Subdevice properties panel will indicate the link status, SFP module type, as well as the LLDP partner.

NOTE: The PWVIA DIN P8 will work with 1000BASE-SX, 1000BASE-LX (1Gbps) and 10GBase-SR and 10GBase-LR (10Gbps) fiber modules. The PWVIA DIN P16 will work with only 1000BASE-SX, 1000BASE-LX (1Gbps) modules.

The PWVIA DIN P8 also support SFP+ Direct Attach cables, both active and passive. This is often the easiest and lowest-cost solutions to connect multiple switches if they are close together.

When connecting a VIA to another manufacturer's switch using fiber, please bear in mind that some switches check the manufacturer's ID, as announced by the SFP module, and will only connect to a matching brand. VIA switches do not perform a manufacturer's ID check, and should work with any SFP module meeting the criteria above (Cisco, Finisar, Netgear, etc.)

APPENDIX 2: VIRTUAL LOCAL AREA NETWORK (VLAN)

A VLAN (Virtual Local Area Network) is a group of ports on the switch (or switches) that are configured to pass traffic to one another, but not to ports on any other VLAN. When multiple VLANs are established, some ports on the switch may need to be configured specifically to pass all VLAN traffic, to ensure overall traffic is routed correctly.

This feature allows the user to arrange lighting consoles, gateways and other network gear into groups of equipment. The usual purpose is to minimize unnecessary traffic to the equipment, or to segregate different types of equipment (lighting, audio, video) so that each network does not get flooded with superfluous data.

DEFINITIONS

The following terms are paired interchangeably in this manual: Normal and Untagged; Uplink and Tagged.

Normal/Untagged ports belong to a specific VLAN as configured by the user, and will only pass traffic that belongs to that VLAN. Typically connected to end equipment.

Uplink/Tagged ports pass all network traffic with VLAN “tags” within the VLAN range established for that switch (see Range Configuration below). Typically connected to other switches.

Tag refers to the marker added to (or removed from) the data packet as the packet enters or exits from a Normal/Untagged port on the switch. The “Tag” determines which VLAN the data packet is assigned to.

Management VLAN refers to the VLAN that the switch’s management processor is assigned to use. Care must be taken that the Management VLAN is used by at least one Normal/Untagged port on the switch, or the ability to configure the switch may be lost. It is strongly recommended that the Management VLAN be identical to the VLAN Range Start.

VLAN ID (ID#) is assigned to Normal/Untagged ports and determines which VLAN that port operates within.

A Normal/Untagged port may only be associated with one VLAN ID# at a given time.

SOFTWARE CONFIGURATION OF VLANs

VLANs may be configured using Pathscape software. Refer to the Pathscape documentation for in-depth configuration instructions.

When using software to configure the switch, make sure your computer is connected to a Normal (Untagged) port set to the same VLAN ID# as used by the management processor. Failure to do so will prevent configuration from being applied.

VLAN GUIDELINES

Plan the VLAN layout first. The creation of a map of the network, showing which devices to associate with which VLAN, is strongly recommended prior to configuration.

Generally speaking, ports connected to end devices will be configured as Normal/Untagged and given a VLAN ID#.

Ports connected to other VIA switches will typically be set as Uplink/Tagged, so multiple VLANs may be forwarded between switches, or when a VLAN must be forwarded through an intermediate switch (where that VLAN is not in use) on to a third switch beyond. It is possible to set the ports to Normal/Untagged, and given a VLAN ID#, in cases where it’s desirable to pass only one VLAN between switches, but this is not a normal practice.

When configuring VLANs, remember that each switch must be uniquely identified on each VLAN in use on that switch. By default, only the management VLAN is automatically assigned an IP and subnet mask. All other VLANs default to a null IP address value (0.0.0.0). Use the Network Configuration options available from the VLAN configuration screen to configure the desired IP settings for each VLAN.

APPENDIX 3: PLANNING CHARTS

VLAN PLANNING CHART

VLAN ID #	1	2	3	4
Label				
IP Address				
Subnet Mask				
Default Gateway				
IGMP Snooping				
IGMP Querier				
DHCP Server				
Art-Net Alternate Mapping				
QoS Level				

VLAN ID #	5	6	7	8
Label				
IP Address				
Subnet Mask				
Default Gateway				
IGMP Snooping				
IGMP Querier				
DHCP Server				
Art-Net Alternate Mapping				
QoS Level				

VLAN ID #	9	10	11	12
Label				
IP Address				
Subnet Mask				
Default Gateway				
IGMP Snooping				
IGMP Querier				
DHCP Server				
Art-Net Alternate Mapping				
QoS Level				

VLAN ID #	13	14	15	16
Label				
IP Address				
Subnet Mask				
Default Gateway				
IGMP Snooping				
IGMP Querier				
DHCP Server				
Art-Net Alternate Mapping				
QoS Level				

SWITCH PLANNING CHARTS

SWITCH LABEL:		
Base IP:	Subnet:	Gateway:
QoS (Off/Standard/Dante):		
VLAN (Enable/Disable):	Range:	Management ID#:
Art-Net Alternate Mapping (On/Off - On is default):		

SWITCH LABEL:		
Base IP:	Subnet:	Gateway:
QoS (Off/Standard/Dante):		
VLAN (Enable/Disable):	Range:	Management ID#:
Art-Net Alternate Mapping (On/Off - On is default):		

PORT	1	2	3	4	5	6	7	8	9	10
Connected Device										
Normal/ Tagged(Uplink)										
VLAN ID#										
Art-Net Trap & Convert										
PoE Max Allocation										
Link Mode										
SFP/SFP+ Type	☒	☒	☒	☒	☒	☒	☒	☒		

PORT	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Connected Device									
Normal/ Tagged(Uplink)									
VLAN ID#									
ArtNet to sACN									
PoE Max Allocation									
Link Mode									
SFP Type	☒	☒	☒	☒	☒	☒	☒	☒	☒

PORT	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**
Connected Device									
Normal/ Tagged(Uplink)									
VLAN ID#									
ArtNet to sACN									
PoE Max Allocation									
Link Mode									
SFP Type	☒	☒	☒	☒	☒	☒	☒		

APPENDIX 4: EAPS & RSTP - “RING PROTECTION”

Ethernet wiring schemes are based on a ‘star’-wiring topology. Ring (or loop) data wiring – where the last device in a chain is wired back to the first device without RSTP or EAPS setup will quickly ‘break’ your network. **Only one data path between any two devices is allowed.**

Pure star-wiring layouts leave your network prone to a single point of failure. Unlike DMX512 networks, passive data “thru” connections are not possible with Ethernet. A severed cable or power loss to a switch can mean the loss of some or even all show control.

Ring Protection allows the deliberate – and designed – use of a ring wiring system for Ethernet communications. With EAPS or RSTP enabled, VIA switches ignore data traffic on one segment of the ring, while monitoring the integrity of the remaining connections. If an interruption is detected, the unused ring segment is activated and full communication is restored.

Ethernet Automatic Protection Switching (EAPS) uses dedicated tagged ports whereas **Rapid Spanning Tree Protocol (RSTP)** can use any two ports on a switch. Fail-over time when using EAPS on dedicated ports is between 50 and 75 milliseconds, or two to four DMX packets.

Using RSTP, the healing process can take a second or two. Unlike EAPS, RSTP only requires you to turn on the feature on all the switches in the network. No further dedicated port configuration or special wiring considerations need to be adhered to. VIA will block data flow on redundant links and report “**Blocked by RSTP**” in the link status. The algorithm that decides which ports to block is based on a stringent set of rules that ensure the fastest network possible.

REQUIREMENTS AND LIMITATIONS

VLANs must be enabled to use Ring Protection. EAPS uses a dedicated VLAN to monitor the integrity of the ring. By default, VLAN 4094 is used. The Ring Protection VLAN must be outside of the established VLAN range.

Only ports 15 through 18 (**PWVIA DIN P16**), and ports 7 through 10 (**PWVIA DIN P8**) may be used with this feature.

EAPS works with VIA switches only. Switches from other manufacturers can co-exist on the network, but should not be placed in-line with the ring.

DEFINITIONS FOR EAPS

Master switch monitors the integrity of communications. **Only one switch on the network may be configured as the master.**

Transit switches receive and forward the ring monitoring packets. **All switches other than the Master must be set as transit switches.**

Primary port is the main (active) UPLINK connection link on the Master switch, joining to the rest of the network. All transit switches must also have one port configured as the primary. Only ports 15 through 18 are available to be used as the primary port (PWVIA DIN P16) or ports 7 through 10 (PWVIA DIN P8).

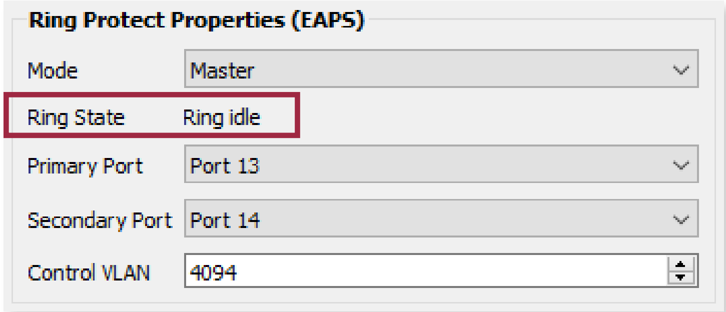
Secondary port is an UPLINK port “ignored” (logically blocked) by the Master switch to break the ring topology. All transit switches also must have one port configured as the secondary port. The secondary port is actively used on transit switches. Only ports 15 through 18 are available to be used as the secondary port (PWVIA DIN P16) or ports 7 through 10 (PWVIA DIN P8).

Control VLAN is a unique VLAN ID dedicated to monitoring the health of the network. All switches must use the same control VLAN. The default is VLAN ID 4094.

NOTE: Ring Protection wiring topology is not structured. Primary ports can be connected to either the Primary or Secondary port on the next VIA.

SOFTWARE CONFIGURATION OF RING

- Start with the redundant wiring segment unplugged.
- Connect the computer running Pathscape to one of the end switches, in the wiring chain.
- Configure the switch that is physically furthest away on the chain. Work backwards until reaching the closest switch.
- Now plug in the redundant wiring segment. Check the **Ring State** property under Ring Protect Properties (EAPS) section in Pathscape.



Ring Protect Properties (EAPS)

Mode	Master
Ring State	Ring idle
Primary Port	Port 13
Secondary Port	Port 14
Control VLAN	4094

- If the "Failed" message does not clear, unplug the redundant segment and check the port settings of each switch for misconfiguration.

APPENDIX 5: QoS SETTINGS

Quality of Service priorities are determined by the Differentiated Services Code Point (DSCP) field contained in each data packet header. DSCP values may range from 1 to 64, and are mapped to four egress (output) queues. The egress queues are, in turn, numbered from 1 (Best Effort) to 4 (Highest Priority).

The DSCP mappings and related QoS settings used by VIA switches is shown in the following table:

QoS Setting	Description
Disabled (default)	Disables QoS-based routing. All traffic is treated equally.
QoS Standard	Queue 1: DSCP values 1-16 Queue 2: DSCP values 17-32 Queue 3: DSCP values 33-48 Queue 4: DSCP values 49-64 A weighted fair queuing algorithm is used to prevent the starvation of lower queues by higher priority traffic.
Dante Strict	Queue 1: All DSCP values except: Queue 2: DSCP 8 Queue 3: DSCP 46 Queue 4: DSCP 56 Queue 3 and 4 are handled by strict priority, while the two lower queues are handled by the weighted algorithm.

APPENDIX 6: ELECTRICAL, COMPLIANCE & OTHER INFORMATION

ELECTRICAL INFORMATION

PWVIA DIN P16 RJ45 SFPSLOT POE

- 20-50 VDC power input, 10W maximum (Switch only)
- 48-50 VDC power input, 190W maximum (including 180W distributed to up to 12 PoE devices)
- Class 3 PoE on ports 1-12 (maximum 15.4W per port)

PWVIA DIN P8 RJ45 SFPSLOT POE

- 20-50 VDC power input, 10W maximum (Switch only)
- 48-50 VDC power input, 130W maximum (including 120W distributed to up to 8 PoE devices)
- Class 3 PoE on ports 1-8 (maximum 15.4W per port)

COMPLIANCE

- ANSI E1.31 sACN - Streaming ACN
- IEEE 802.3 Ethernet
- IEEE 802.3af - Class 3 Power-over-Ethernet (with external supply)
- IEEE 802.1AB Link Layer Discovery Protocol
- IEEE 802.1Q VLAN Support
- IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
- California Title 1.81.26, Security of Connected Devices
- CE
- RoHS 2011/65/EU:2015/863

PHYSICAL

PWVIA DIN P16 RJ45 SFPSLOT POE

- 1.08 lbs (0.49 kg)
- 8” W x 4” H x 3.1“ D x (203mm W x 103mm H x 79mm D)
- Operating Conditions: 14°F-113°F (-10°C to +45°C); 5-95% relative humidity, non-condensing

PWVIA DIN P8 RJ45 SFPSLOT POE

- 1.05 lbs (0.47 kg)
- 6.25” W x 4”H x 2.9“ D (159mm W x 102mm H x 74mm D)
- Operating Conditions: 14°F-113°F (-10°C to +45°C) 5-95% relative humidity, non-condensing