

cognito² LIGHTING CONTROL CONSOLE

choreo[™] ARCHITAINMENT LIGHTING CONTROLLER



Models 0700-71XX, 0700-73XX
Running November 2020 Firmware or later

User Guide Addendum

December 2020



Pathway Connectivity
1439 17 Ave SE • Calgary, AB • T2G 1J9
+1 (403) 243-8110
support@pathwayconnect.com





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

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media, printed materials and "on-line" or electronic documentation (the "Software Application") constitutes an unpublished work and contains valuable trade secrets and proprietary information belonging to Pathway and its licensors.

WARNING ABOUT 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 THIS DOCUMENT	1
SECURITY	1
BACKGROUND INFORMATION	1
WHAT THIS MEANS TO YOU	1
HOW THIS AFFECTS CHOREO & COGNITO	2
SECURITY DOMAINS	3
RED PADLOCK -  Unsecured Device	3
AMBER PADLOCK -  Secured Device not in the Current Domain	3
AMBER PADLOCK -  Locally Secured.....	3
GREEN PADLOCK -  Secured Device in Current Domain	3
EMPTY SECURITY DOMAIN CELL – Firmware version prior to 5.0 - device shipped prior to January 1, 2020	3
CREATING A SECURITY DOMAIN.....	4
ADMINISTERING A DOMAIN	8
MANAGE SECURITY DOMAIN.....	8
RECOVERING A DOMAIN	15
RETAINING DEVICE SETTINGS FROM UNKNOWN DOMAINS	16
USING OLDER VERSIONS OF PATHSCAPE WITH NEW DEVICES.....	16
LOCAL SECURITY - USING CHOREO/COGNITO² WITHOUT PATHSCAPE.....	17
INTRODUCING PATHWAY ssACN (Secure sACN)	18
DOMAIN AUTO ssACN PASSWORD.....	18
CUSTOM ssACN PASSWORD	18

CHOOSING PATHWAY ssACN AS NETWORK PROTOCOL.....	19
MANAGING PATHWAY ssACN PASSWORDS	20
USING ssACN ON CHOREO/COGNITO	22
sACN / ssACN PRIORITY.....	23
ADDING NSB WALL STATIONS TO CHOREO/COGNITO	24
SOFTWARE (PATHSCAPE) CONFIGURATION.....	26
DEVICE PROPERTIES.....	26
PATHWAY SECURITY DOMAIN.....	26
BASIC PROPERTIES	26
DEVICE INFO	27
NETWORK PROPERTIES	27

ABOUT THIS DOCUMENT

This document is an addendum to the full Choreo/Cognito² User Guide. This guide describes features now available with current firmware release **November, 2020**.

These features include:

- Supports Choreo/Cognito² joining Pathscape Security Domain
- Supports Pathway ssACN (Secure ACN) Network DMX protocol transmission
- sACN / ssACN Priority Level is configurable

For general use instructions, consult the Choreo/Cognito² User Guide.

SECURITY


BACKGROUND INFORMATION

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

The law requires us to either supply a unique password for our products (see **Local Security** below) or requires the users to change the password before being able to use it (See **Creating a Security Domain** below). With Pathscape V3, we provide features that protect our products from unauthorized access or use by enforcing passwords. Furthermore, Pathway Connectivity does not collect or store personal information on our devices.

WHAT THIS MEANS TO YOU

1. When using products shipped after January 1, 2020, Pathscape will require a single password to allow configuration of all the devices on your network. As of the release of Pathscape V4, all Pathway Connectivity products can be upgraded to firmware version 6.x. It is suggested you upgrade your devices to take advantage of the most recent security improvements.
2. Products shipped before January 1, 2020, devices with version 3.x and 4.x firmware will continue to function without passwords using either Pathscape version 3 or 4.
3. All products shipped after January 1, 2020 may only be configured using Pathscape 4.
4. Products shipped after January 1, 2020 cannot be downgraded to earlier password-free firmware.

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

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

5. Products that are fully configurable from the front panel can create their own unique password. Only with network configured products will you need to type a password; one password for all devices on the network.
6. You will be encouraged to print or save a recovery key in case you lose the password. Do so when setting up your Security Domain. It is the **only chance** you'll get to save/print/see this Recovery Key.
7. If you lose the password and lose the recovery key, you will manually have to factory default each device on the network.

See the resource section of the Pathway website for a comprehensive document describing how to manually factory default all our devices.

8. The complete network configuration may be saved without a password before factory defaulting devices. Applying the saved configuration will require a new password to be set for the network.
9. Configuring our devices to receive unsecured protocols such as sACN and 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.


HOW THIS AFFECTS CHOREO & COGNITO











With the November 2020 firmware and later, Choreo and Cognito² can join a Pathscape Security Domain (see following pages) using the touchscreen. This allows the use of Pathway ssACN (Secure sACN). By default, the Choreo/Cognito² will ship with Local Security enabled.

With these new features, your lighting network is safe and secure from potential threats right from the source, all the way to the downstream fixtures.

SECURITY DOMAINS

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

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

AMBER PADLOCK - Secured Device not in the Current Domain

Devices that have been added to a security domain will appear with an amber padlock. These firmware v5 devices will allow you to read all their properties and even save a show file with the network setup, but the properties are Read-Only. You will have to login to the domain to set any properties. (See **Login procedure** below.)

AMBER PADLOCK - Locally Secured

You may also see **Locally Secured** beside an amber padlock. By default, Choreo and Cognito² (with November 2020 or later Firmware) will be Locally Secured.

When Locally Secured, the device allows front-panel-only configuration. To gain read/write privileges with Pathscape, you **must add it to a Security Domain** using Pathscape. See below for details.

GREEN PADLOCK - Secured Device in Current Domain

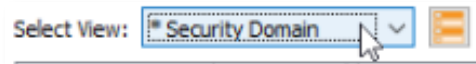
Once you have logged into a Security Domain with a password, any device in your domain will appear with a green padlock and all their properties will be Read/Writeable.

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 3 will be able to read and write properties exactly like Pathscape 2. If you upgrade to v5 firmware the device will appear with a red padlock and you will need to add it to a domain before you can use it.

CREATING A SECURITY DOMAIN

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

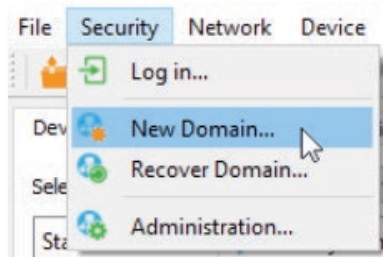


- Each device running V5 or later firmware will have a **Red “Unsecured”** value in the **Security Domain** column.

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:

Admin Password:

Retype Admin Password:

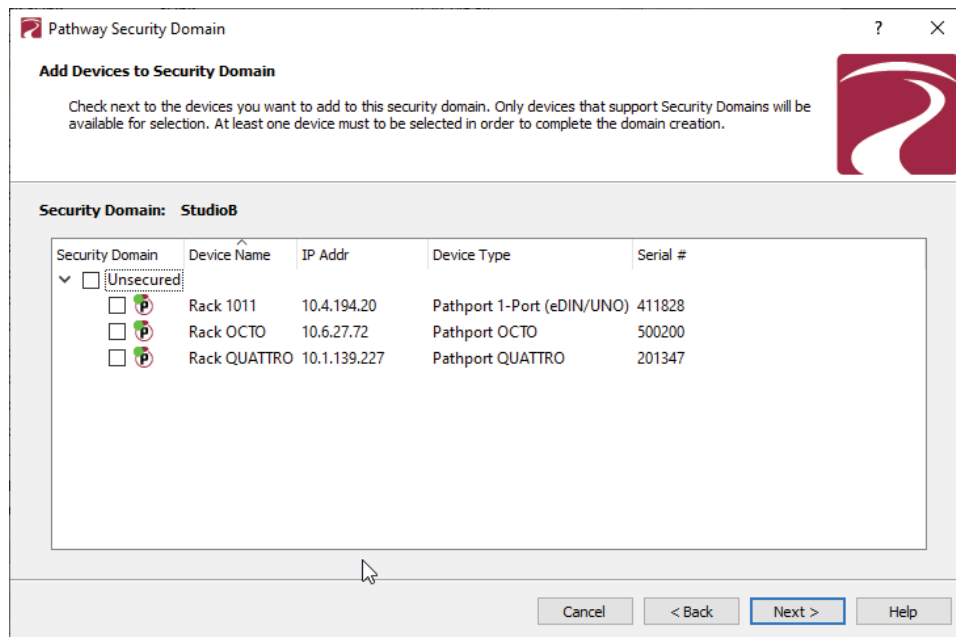
User Password:

Retype User Password:

☐ Show Text

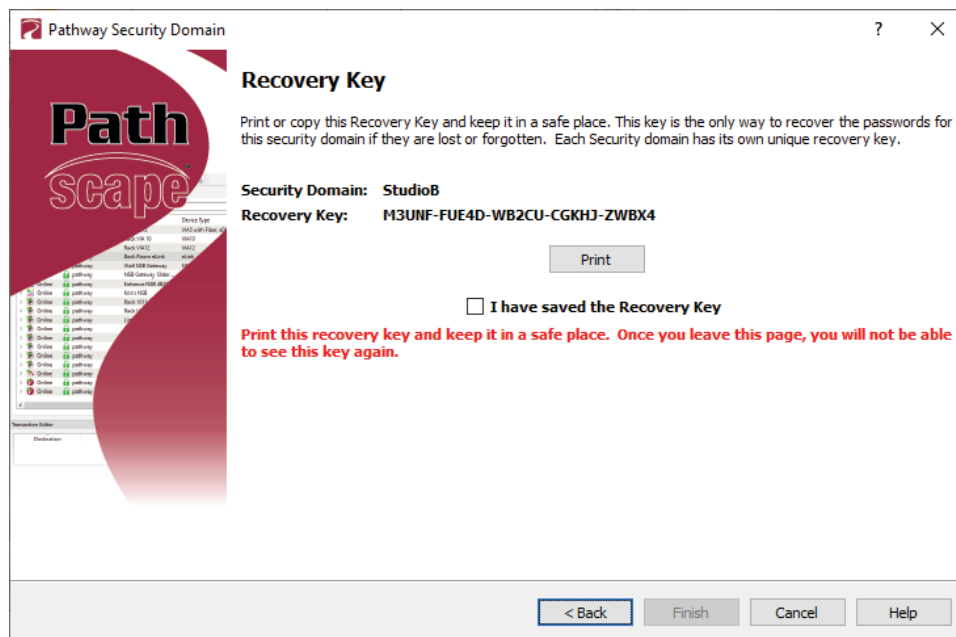
- Enter the new **Domain Name** and **Administrator** and **User passwords**, then click **Next**.
 - The **Administrator** can change passwords, factory default devices and add or remove devices from the domain.
 - The **User** can change device properties and save and restore show files, but cannot 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 then click **Next**. If you wish to add some but not all devices to this domain, click on the checkbox next to each device you’d like to add, and then click Continue.

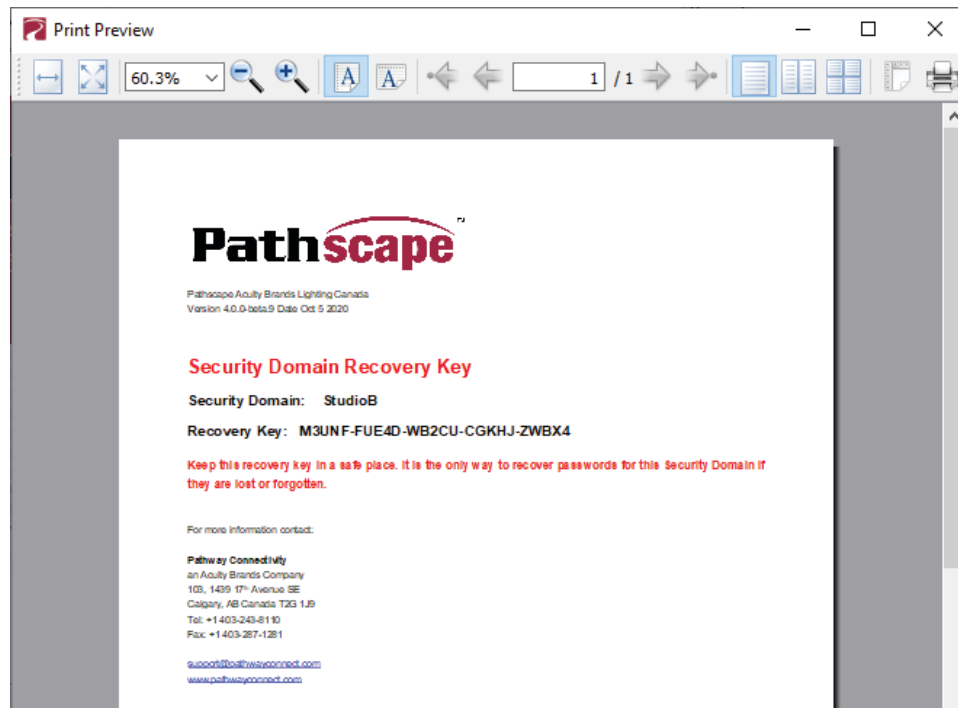


- The next window will show the **Recovery Key**. This key will allow you to recover Security Domain access should the passwords be lost or forgotten.

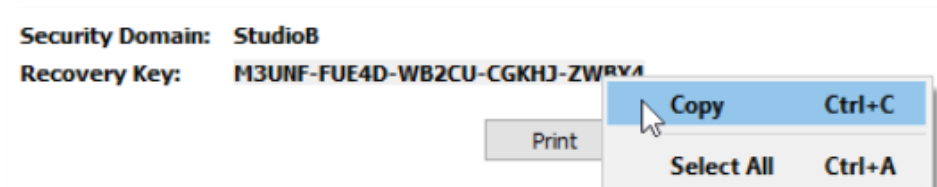
It is extremely important to keep a record of this Recovery Key, as this is the only time it will be shown to you. Print the Recovery Key.



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









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




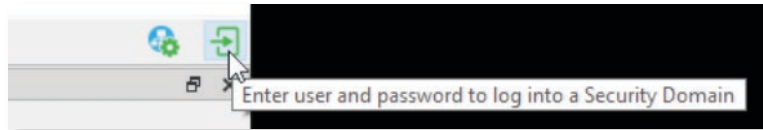
- In order to proceed, you **must click the checkbox** acknowledging you have printed or saved the Recovery Key in some way.



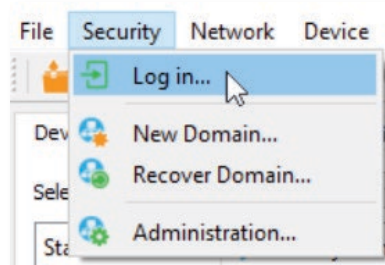
- Click **Finish** and the window will close, and the devices will be added to the domain. The devices will have an **amber padlock** and their properties will be read-only.

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

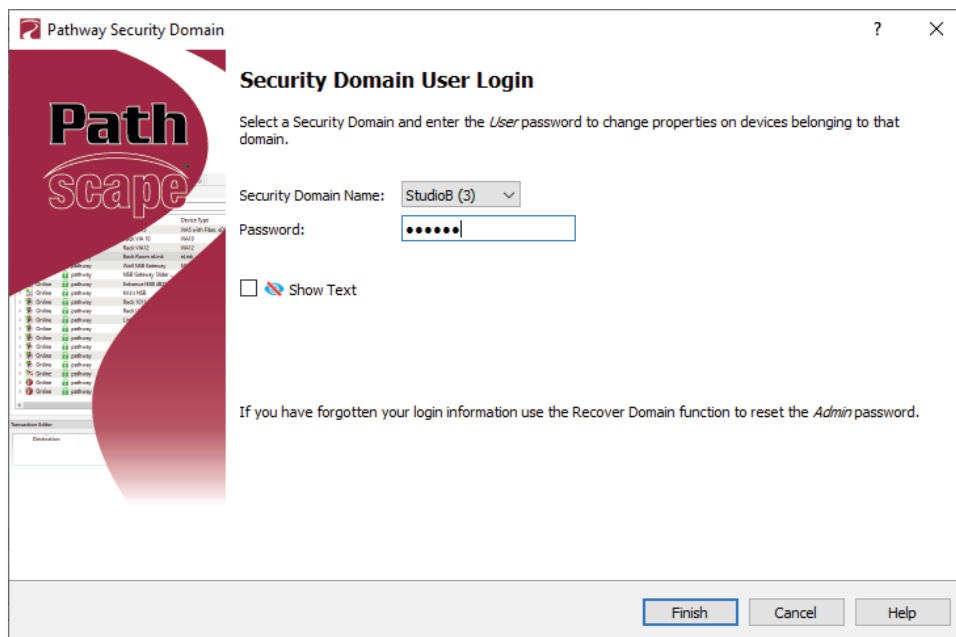
- To configure the devices, you must log in to the domain **as a user** by pressing the  Log In button in the toolbar. **Note:** The **Security Toolbar** option under the **Window** menu must be checked





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

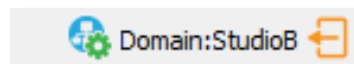


- Enter the **User** password for the Security Domain that was just created, and click **Finish**.



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

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

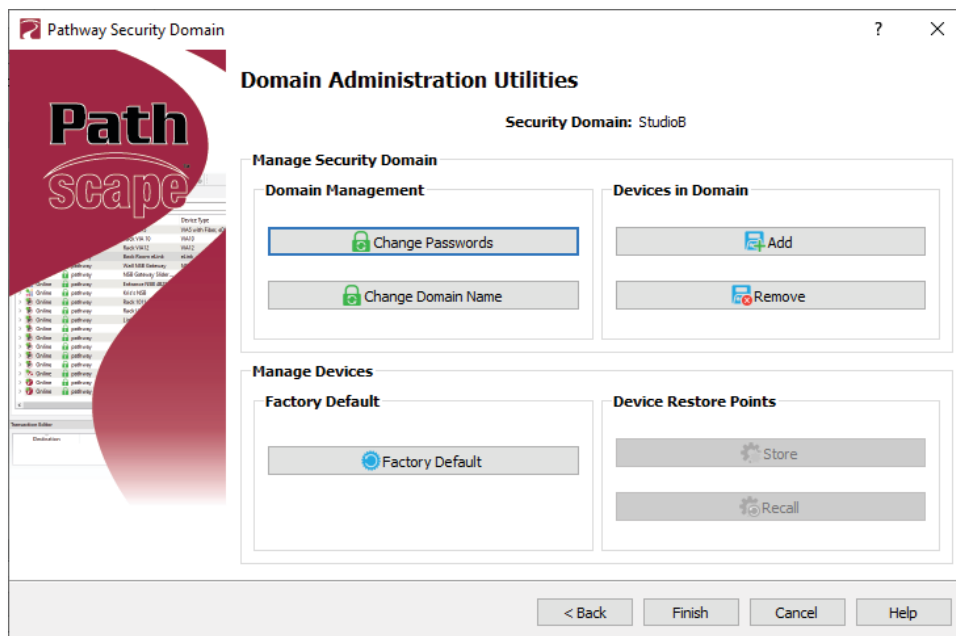


ADMINISTERING A DOMAIN

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



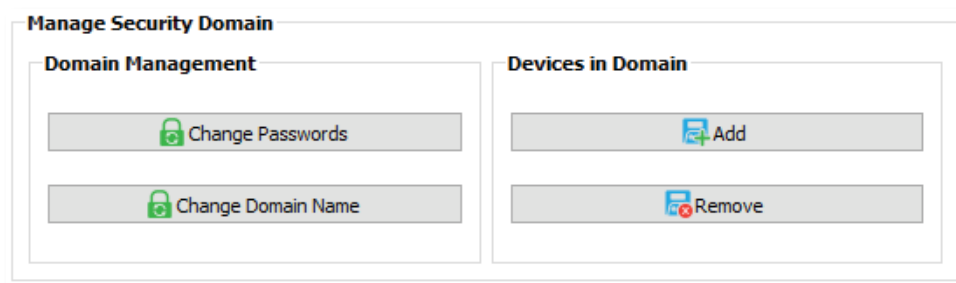
Enter the **Admin** password for the Security Domain, and the **Domain Administrator Utilities** window will appear.



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

MANAGE SECURITY DOMAIN

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



DOMAIN MANAGEMENT



CHANGE PASSWORDS

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



Change Security Domain Passwords

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

Domain Name: **Studio8**

Admin Password:

Retype Admin Password:

User Password:

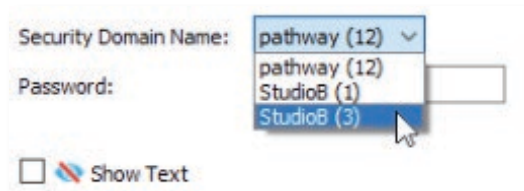
Retype User Password:

☐ 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 coincidentally 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

pathway (12)
pathway (12)
Studio8 (1)
Studio8 (3)

You will have to remove the devices that are on the old domain, then add them to the new domain using the new password.

You can remove them using the  **Remove** button in the **Domain Administration Utilities** menu (see below for details).

The number in parentheses after the name is the number of devices that are in that domain. This should help you identify which is the old domain. Log into the old domain using the old password and remove the devices. When they come back online, they will appear as  **Unsecured**. Add them to the new domain using the new password.

CHANGE DOMAIN NAME

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



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

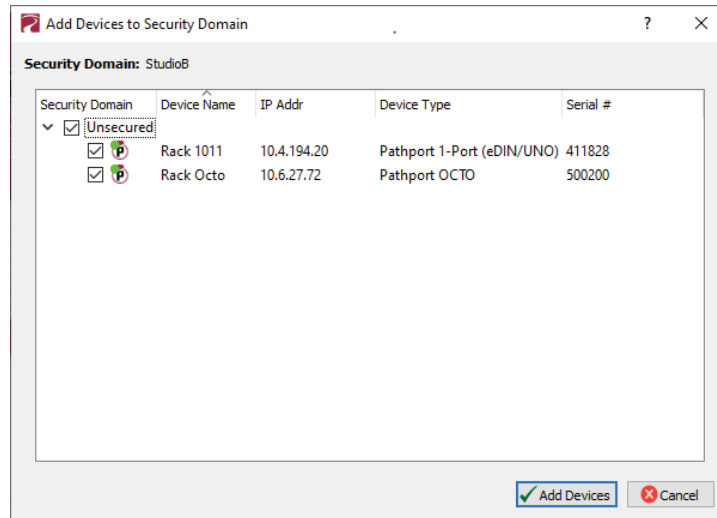
The window will close, and you will be logged out of the current domain, and the Domain Name will be changed to the new value. **You will have to log into the Domain again** to make any further changes.

Note that changing the domain name **does not** generate a new Recovery Key. The original key is still valid, as it is only generated at the time of the domain's creation. It is advised to make note of the changed domain name and store it in the same location as the Recovery Key, so the domain can be recovered in the future if necessary.

DEVICES IN DOMAIN



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

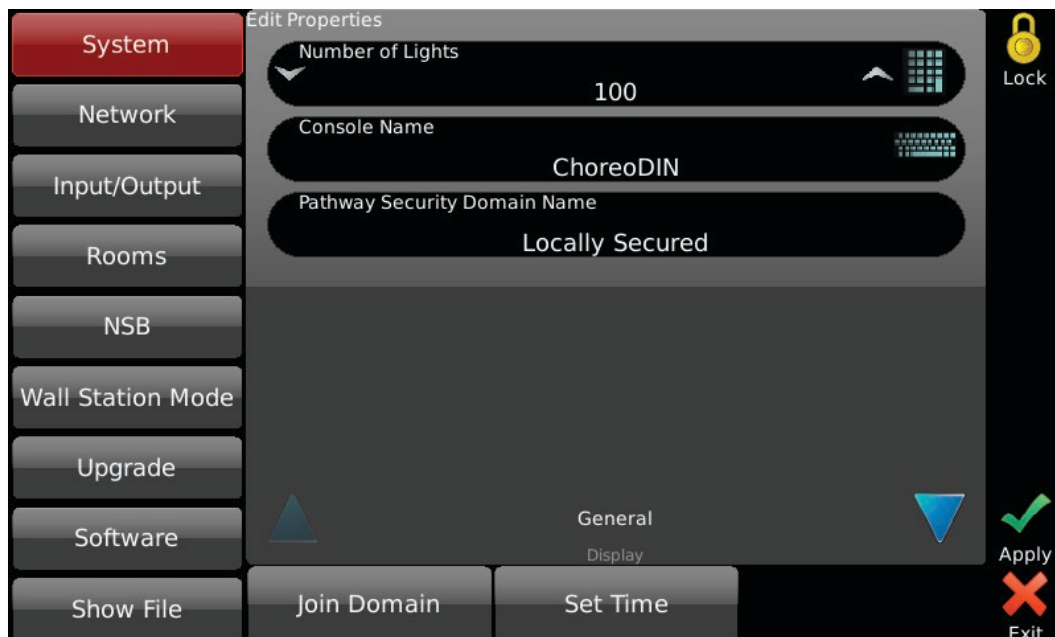


Click on the checkboxes next to the devices you want to add to the Domain, and click the **Add Devices** button. To add all the listed devices, click the top checkbox next to “Unsecured” which will auto-check all the devices’ checkboxes.

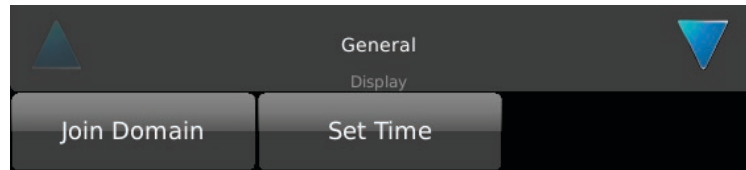
ADDING CHOREO OR COGNITO² TO A SECURITY DOMAIN

Choreo or Cognito² will not appear in the above list by default. To add Choreo or Cognito² to a Security Domain, you must first put the controller in “**Join**” mode.

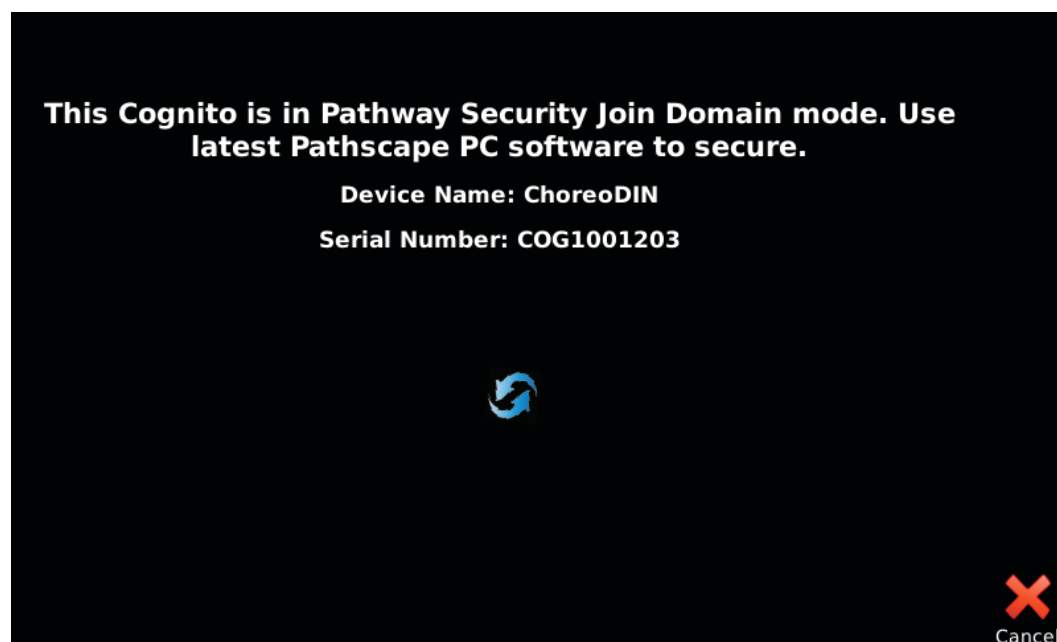
- On the front panel, tap on the  **Setup** button to access the main menu.






- Tap on the **System** button, if not already selected.
- At the bottom of the window, tap the **Join Domain** button.




- The **Join Domain** screen will then appear, with a spinning cursor. In this mode, the Choreo/Cognito² is waiting for you to complete the Join Domain process in Pathscope. It will display the Device Name and Serial Number to help you identify the correct device in Pathscope's device list.

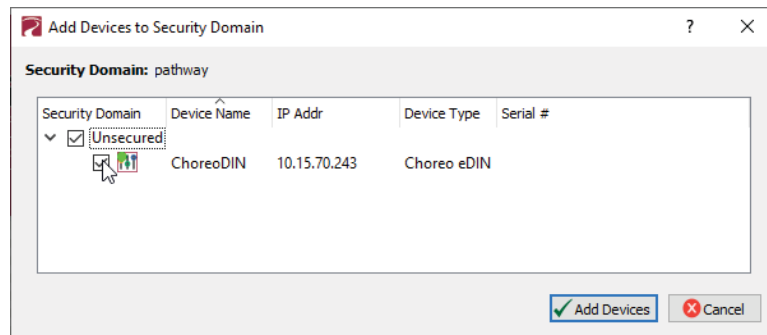


- Open Pathscope. You should see your device in the Device View, as  **Unsecured**. Confirm the device's Name and Serial Number.



Status	Security Domain	Device Name	Device Type	IP Addr
 Online	 Unsecured	ChoreoDIN	Choreo eDIN	10.15.70.243

Device Info	
Device Type	Choreo eDIN
Network Interface	Ethernet 4
Firmware Version	2.0 Nov 6 2020 22:07
Serial Number	COG1001203

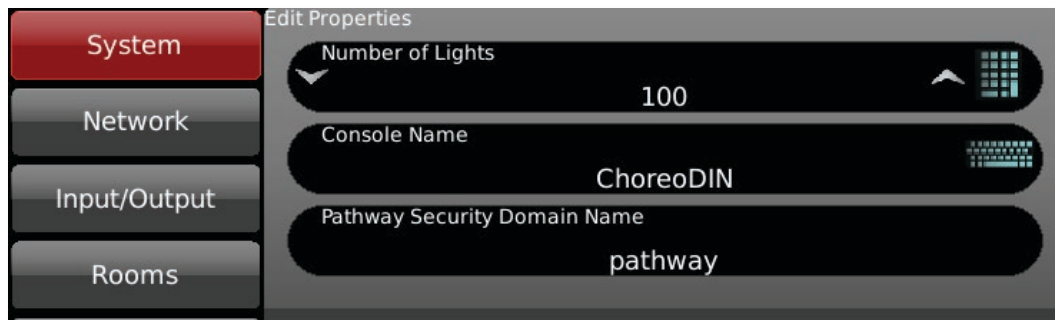
- Log into your Domain Admin as shown above, and click the  **Add Devices** button. You will see the Choreo/Cognito² in the list of available devices to add. Select it and click **Add Devices**.



- Click Finish in the Admin window. Your device is now added to the Domain. The controller's screen will return to the **Setup** menu.

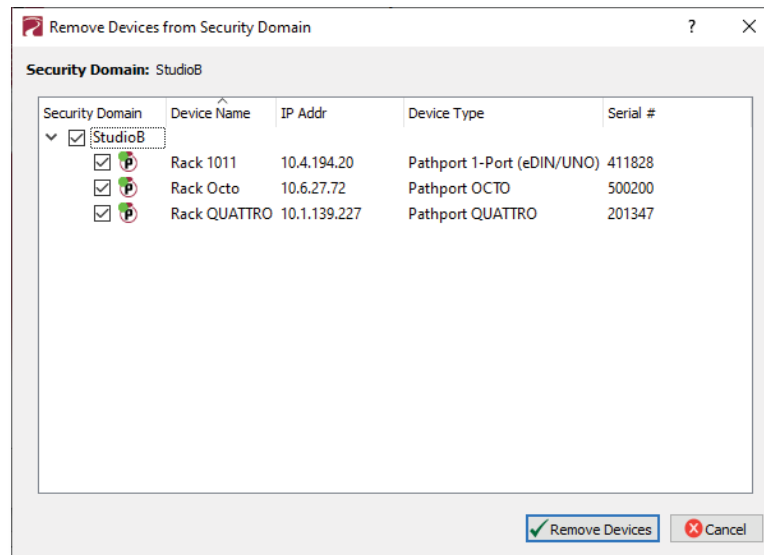
Status	Security Domain	Device Name	Device Type
 Online	 pathway	ChoreoDIN	Choreo eDIN

- Under the **System** menu | **General**, notice the field **Pathway Security Domain Name** now shows the name of the domain, in this case “pathway”.




REMOVE

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



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

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

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

RECOVERING A DOMAIN

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

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



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



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

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



RETAINING DEVICE SETTINGS FROM UNKNOWN DOMAINS

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



Once they reappear in Pathscape with a red padlock, add the devices to a Security Domain, then open the show file and **Send All Transactions** to restore the network configuration and patch.

USING OLDER VERSIONS OF PATHSCAPE WITH NEW DEVICES

If you use Pathscape 1 or Pathscape 2 with devices shipped after **January 1, 2020 (Version 5 firmware)**, you will not be able to configure them; **you must use Pathscape 3 or newer**. As a reminder, the device label will appear in the earlier versions of Pathscape as **"Use latest Pathscape PC software to secure"**. Other properties will be shown and are correct, but any attempts to change them will fail.

LOCAL SECURITY - USING CHOREO/COGNITO² WITHOUT PATHSCAPE

Choreo and Cognito² have features that use unsecure protocols. You may not intend to use Pathscape and Security Domains, but “bad actors” could potentially access the device and change the configuration. Therefore, by default, Choreo/Cognito² has Local Security enabled by default from the factory (or once upgraded to November 2020 Firmware or later).

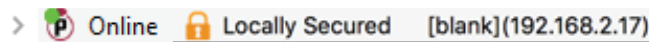
This makes the device configurable only using the front panel only. Additionally, Pathway ssACN (Secure sACN) and use of NSB Wall Stations are not supported when in Local Security mode. If you wish to use these features, it must be added to a **Security Domain**.



All other device functionality remains when in Local Security mode - including transmitting using unsecured DMX-over-Ethernet protocols such as E1.31 sACN, Art-Net and Pathport Protocol.

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.

In Pathscape, this device will be part of the domain “Locally Secured”.



>  Online  Locally Secured [blank](192.168.2.17)

You cannot login to this security domain.

INTRODUCING PATHWAY ssACN (Secure sACN)

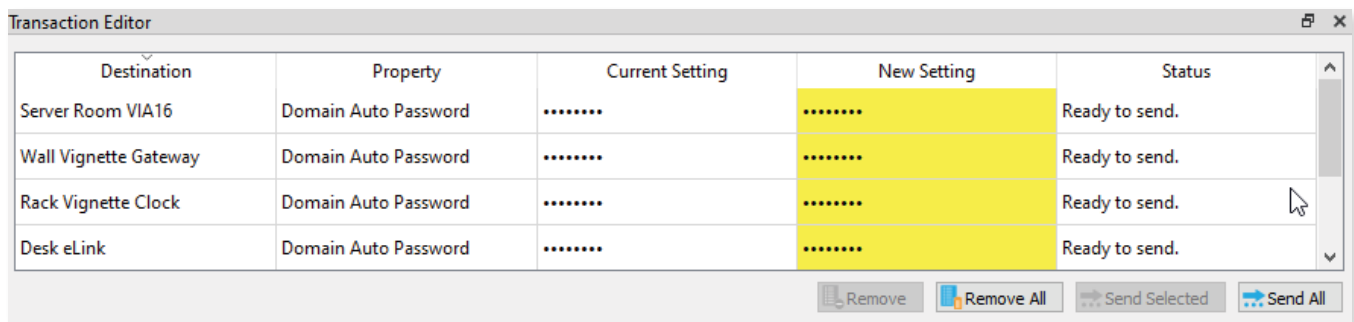
Pathway ssACN (Secure streaming ACN) is a new protocol developed by Pathway using much of ANSI E1.31, but adds a layer of authentication. This feature requires **device firmware version 6.0 or later (Pathport Gateways, Vignette and other devices)** and **Choreo/Cognito firmware version November 2020 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.



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

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

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

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

CUSTOM ssACN PASSWORD

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

This is useful in a few situations:

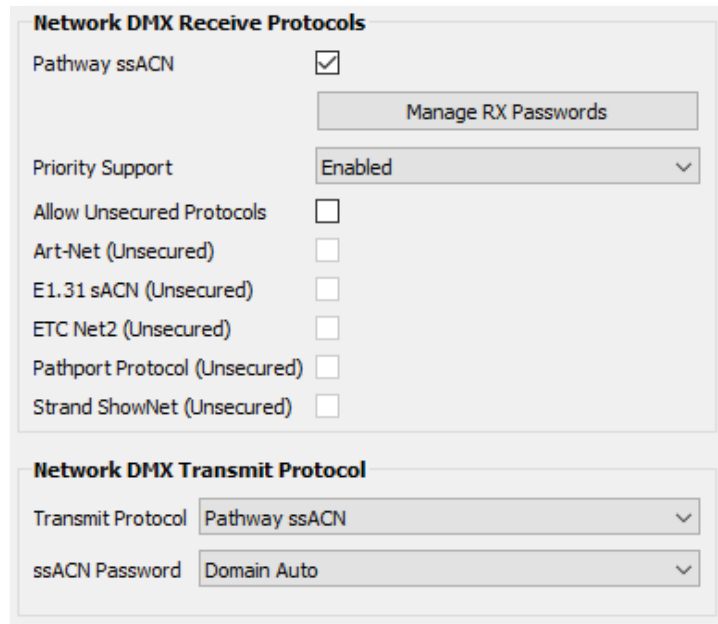
- **If you need to send DMX data across different Security Domains:** specify a custom **ssACN TX password**, and enter the same password on the receiving devices under **ssACN RX passwords**. The receiving devices will then be able to authenticate that data. Domain Auto passwords, as noted above, are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

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

CHOOSING PATHWAY ssACN AS NETWORK PROTOCOL

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

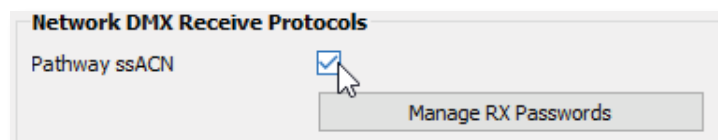
In the relevant devices' **base device** properties, there are two sections called **Network DMX Receive Protocols** and **Network DMX Transmit Protocol**.



The image shows two configuration sections from a software interface. The top section, titled "Network DMX Receive Protocols", contains a checkbox for "Pathway ssACN" which is checked, a "Manage RX Passwords" button, a "Priority Support" dropdown menu set to "Enabled", and several unchecked checkboxes for "Allow Unsecured Protocols", "Art-Net (Unsecured)", "E1.31 sACN (Unsecured)", "ETC Net2 (Unsecured)", "Pathport Protocol (Unsecured)", and "Strand ShowNet (Unsecured)". The bottom section, titled "Network DMX Transmit Protocol", contains a "Transmit Protocol" dropdown menu set to "Pathway ssACN" and an "ssACN Password" dropdown menu set to "Domain Auto".

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

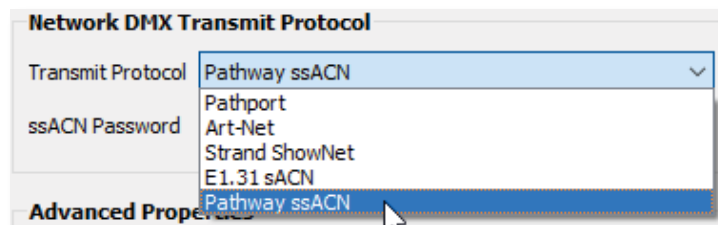
In the **Network DMX Receive Protocol** section, simply check the Pathway ssACN checkbox. We recommend unchecking the Allow Unsecured Protocols checkbox, if previously checked, since end devices can receive **both** ssACN and unsecured protocols if left checked.



This is a close-up of the "Network DMX Receive Protocols" section, specifically focusing on the "Pathway ssACN" checkbox, which is being checked by a mouse cursor. The "Manage RX Passwords" button is also visible below it.

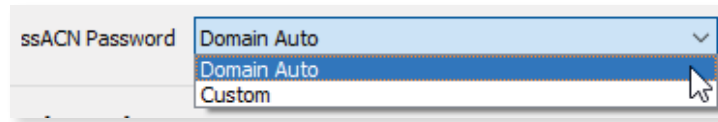
This will ensure the receiving devices will only accept authenticated Pathway ssACN.

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



The image shows the "Network DMX Transmit Protocol" section with the "Transmit Protocol" dropdown menu open. The menu lists several options: "Pathway ssACN" (which is highlighted in blue), "Pathport", "Art-Net", "Strand ShowNet", "E1.31 sACN", and "Pathway ssACN" (repeated at the bottom). A mouse cursor is pointing at the bottom "Pathway ssACN" option. The "ssACN Password" dropdown menu is also visible, set to "Domain Auto".

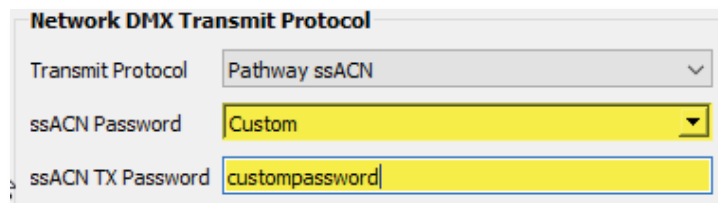
Once you select **Pathway ssACN**, the **ssACN Password** drop-down menu will appear.



A screenshot of a web interface showing a dropdown menu for 'ssACN Password'. The menu is open, showing three options: 'Domain Auto' (selected), 'Domain Auto', and 'Custom'. A mouse cursor is pointing at the 'Custom' option.

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

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



A screenshot of a web interface titled 'Network DMX Transmit Protocol'. It contains three fields: 'Transmit Protocol' (set to 'Pathway ssACN'), 'ssACN Password' (set to 'Custom'), and 'ssACN TX Password' (set to 'custompassword').

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

More on managing ssACN Passwords below.

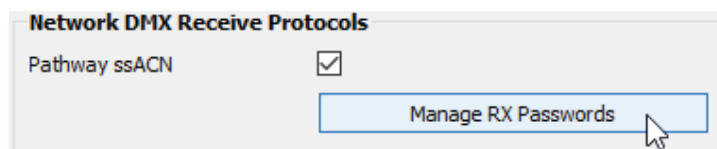
MANAGING PATHWAY ssACN PASSWORDS

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

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

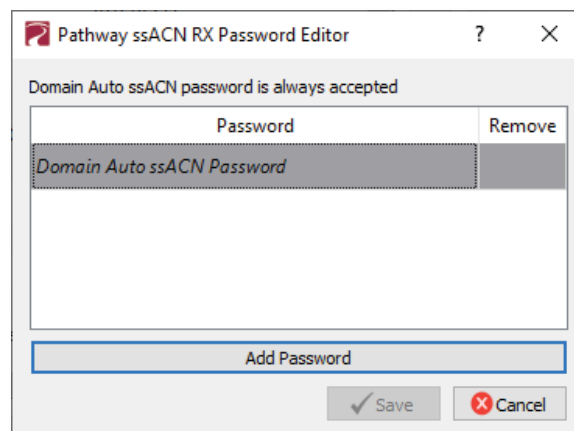
RX (RECEIVE) PASSWORDS

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



A screenshot of a web interface titled 'Network DMX Receive Protocols'. It shows a checkbox for 'Pathway ssACN' which is checked. Below the checkbox is a button labeled 'Manage RX Passwords'. A mouse cursor is pointing at the button.

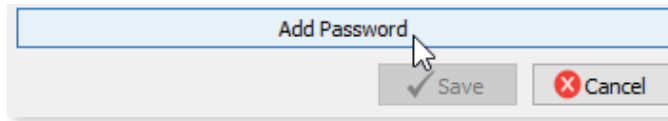
Click it to open the **Pathway ssACN RX Password Editor**.



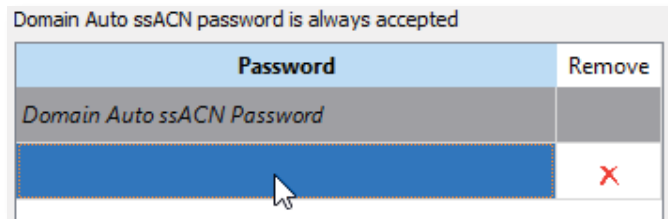
A screenshot of a dialog box titled 'Pathway ssACN RX Password Editor'. It contains a table with two columns: 'Password' and 'Remove'. The first row contains 'Domain Auto ssACN Password' and a button to remove it. Below the table is an 'Add Password' button. At the bottom are 'Save' and 'Cancel' buttons. A message at the top states 'Domain Auto ssACN password is always accepted'.

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

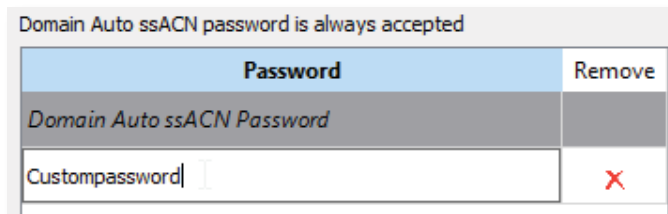
To enter a new password, click the Add Password button.





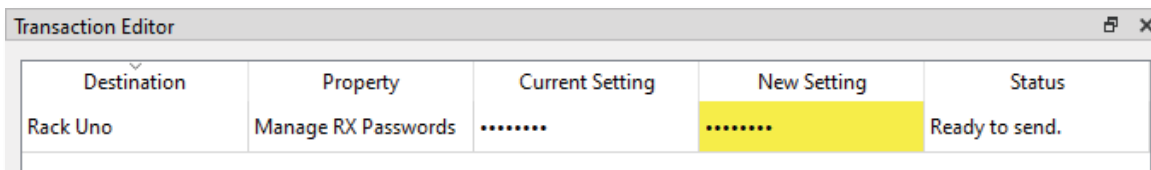
A blank entry will be added to the window.



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



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

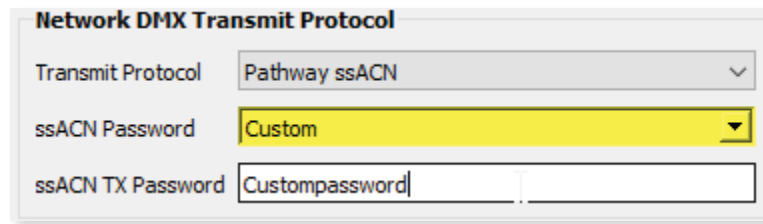


Click the  button to close the window without saving any changes or edits made.

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

TX (TRANSMIT) PASSWORDS

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



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

NOTES ABOUT PATHWAY ssACN

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

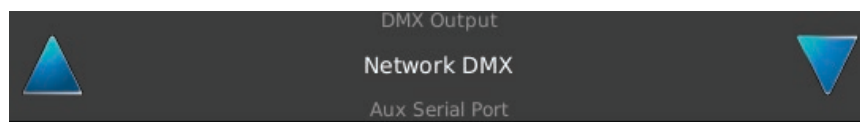
However, receive devices, as shown above, can accept any number of different custom passwords.

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

USING ssACN ON CHOREO/COGNITO



Once Choreo/Cognito² is added to a domain, enable Pathway ssACN by navigating to the **Input/Output** page in the menu and then tapping on the Up/Down arrows to select the **Network DMX** submenu.



Pathway ssACN Universe Offset will be listed alongside the other Network DMX Protocols. By default, it will be set to Off.



Set this offset as you would the other Network DMX Protocols.



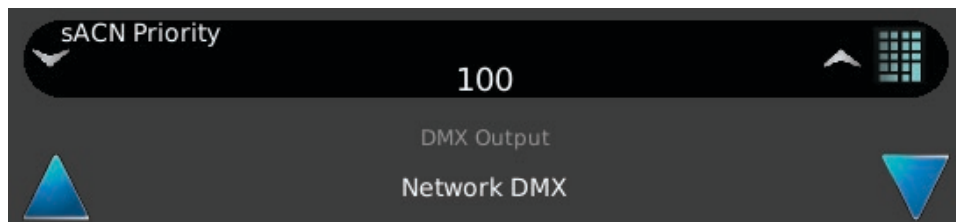
NOTE that Choreo/Cognito² uses the **Domain Auto** ssACN Password only. There is no support for setting Custom ssACN TX Passwords.

sACN / ssACN PRIORITY

Prior to the November 2020 firmware, sACN Priority on Choreo/Cognito² was hard-coded at 100, a typical default value. Now it is possible to specify the sACN or ssACN priority value in the Network DMX menu.

NOTE this value applies to both E1.31 sACN and Pathway ssACN. It is not possible to specify a different value for both protocols.

To configure the sACN Priority, tap on the  **Setup** button to access the main menu, then tap on the **Input/Output** button. Use the Up/Down arrows to select the **Network DMX** submenu.

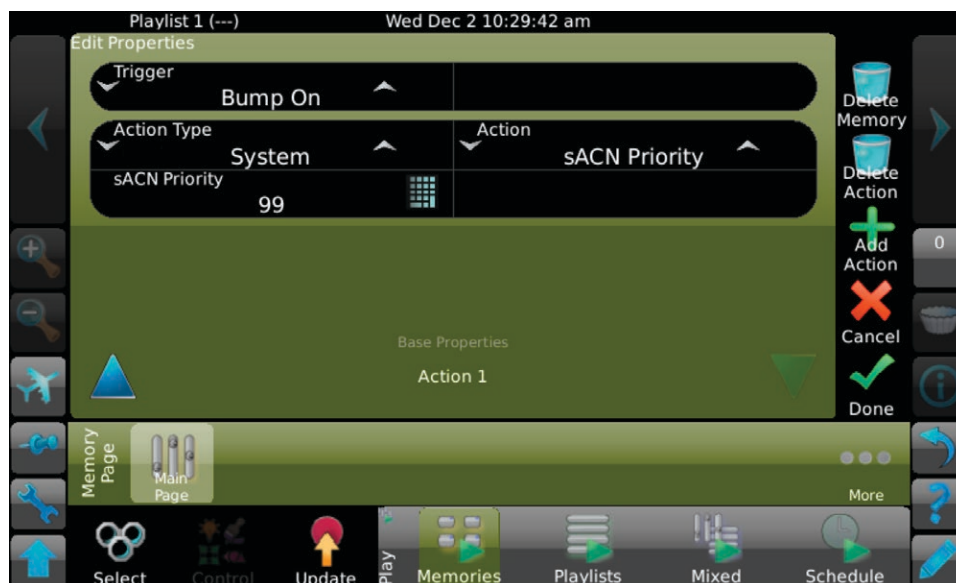


Use the sACN Priority field to set the desired priority.

Cues and Memories can call **Actions** to change the sACN and ssACN Priority.

On Cognito², scroll to **Action Type Cognito** and choose **Action sACN Priority** and set a value.

On Choreo, the Action can be found under **Action Type System**.









ADDING NSB WALL STATIONS TO CHOREO/COGNITO



NSB (Networked Sliders and Buttons) Wall Stations work as before; however with the introduction of firmware version 6.0 for NSB and Choreo/Cognito² firmware November 2020 or later, the controller and wall station(s) to be added **must exist on the same Security Domain**.

All other functionality and configuration remains the same.


- Ensure both the NSB stations to be added as well as the controller are on the same Security Domain. See the above Security section for instructions on **adding** devices to or **removing** devices from a Security Domain.

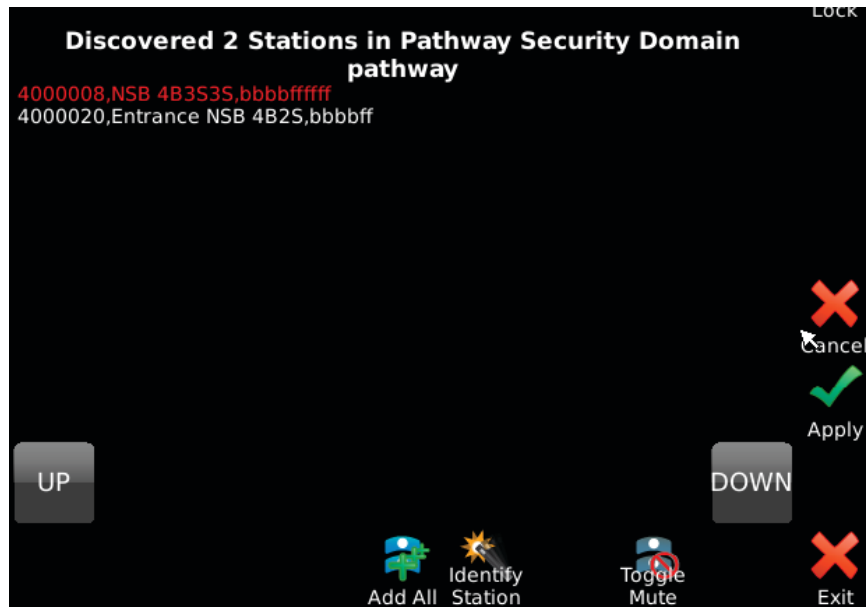
Status	Security Domain	Device Name	Device Type
 Online	 pathway	ChoreoDIN	Choreo eDIN
>  Online	 pathway	Entrance NSB 4B2S	NSB PoE Station
>  Online	 pathway	NSB 4B3S3S	NSB PoE Station

Both the Choreo and NSB Stations are on the same Security Domain "pathway".

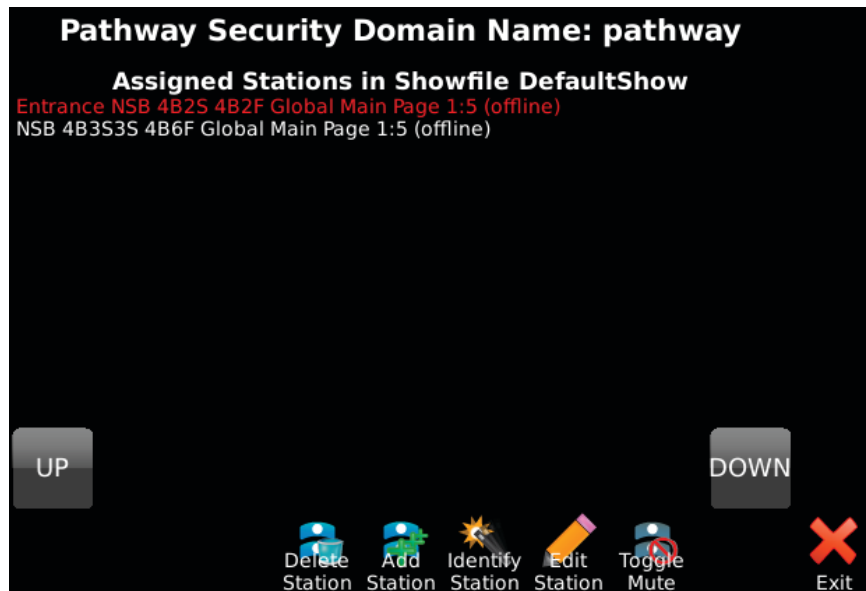
- On the Choreo/Cognito², tap on the  **Setup** button to access the main menu. Tap on the  button. The NSB screen will show the **currently assigned** stations and the current Security Domain name.



- To add a station, tap the  button. The controller will show a list of the NSB stations discovered on the network in the current Security Domain.



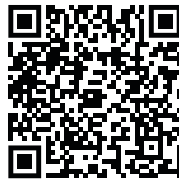
- Tap the  or  buttons to highlight the desired station(s) in **red** and tap the  button to confirm. You can also tap the  to add all discovered stations.



- Edit the stations as per the instructions in the Choreo/Cognito² User Guide.

SOFTWARE (PATHSCAPE) CONFIGURATION

We recommend using Pathscape for configuration of your Pathway devices. 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/index.php/products/software/176-pathscape>. Use the QR Code below to visit the download page.



All configuration of Choreo and Cognito² is done on the device itself. However, from Pathscape, you can change the Device Name if you so choose.

DEVICE PROPERTIES

The following fields are shown in the Device Property Panel in Pathscape. The Device Name is 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

DOMAIN NAME

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

BASIC PROPERTIES

Basic Properties

Device Name

DEVICE NAME

A user-configured, soft label for the Choreo/Cognito² shown in the Device window. If left blank (and by default) the device name displayed will be the device's IP Address.

Setting a Device Name here will be synced to the device and vice-versa (if the Device Name is changed on the device using the front panel, it will be updated here in Pathscape).

DEVICE INFO

Device Info	
Device Type	Choreo eDIN
Network Interface	Ethernet 4
Firmware Version	2.0 Nov 6 2020 22:07
Serial Number	COG1001203

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. Read-only. See the full manual for instructions on updating device firmware.

SERIAL NUMBER

Factory-set unique identifier. Read-only.

NETWORK PROPERTIES

Network Properties	
IP Address	10.15.70.243
Subnet Mask	255.0.0.0

IP ADDRESS

Internet Protocol address (IPv4) of the device. Read-only from Pathscape. Use the controller front panel to configure Network settings.

SUBNET MASK

User-configured subnet mask. Typically, 255.255.255.0 but must be set according to general networking rules. Read-only from Pathscape. Use the controller front panel to configure Network settings.

