UC-AUDIO-POD and UC-AUDIO-HUB

Crestron Flex Pod Wireless Audio Solution

Product Manual

Crestron Electronics, Inc.

The original language version of this document is U.S. English.
All other languages are a translation of the original document.

Regulatory Model: M202109001, M202109002

Crestron product development software is licensed to Crestron dealers and Crestron Service Providers (CSPs) under a limited nonexclusive, nontransferable Software Development Tools License Agreement. Crestron product operating system software is licensed to Crestron dealers, CSPs, and end-users under a separate End-User License Agreement. Both of these Agreements can be found on the Crestron website at www.crestron.com/legal/software_license_agreement.

The product warranty can be found at www.crestron.com/warranty.

The specific patents that cover Crestron products are listed online at www.crestron.com/legal/patents.

Certain Crestron products contain open source software. For specific information, please visit www.crestron.com/opensource.

Crestron, the Crestron logo, and XiO Cloud are either trademarks or registered trademarks of Crestron Electronics, Inc. in the United States and/or other countries. Kensington and Kensington Security Slot are either trademarks or registered trademarks of ACCO Brands Corporation and its subsidiaries in the United States and/or other countries. Bluetooth is either a trademark or registered trademark of Bluetooth SIG, Inc. in the United States and/or other countries. DECT is either a trademark or registered trademark of the European Telecommunications Standards Institute in the United States and/or other countries. Intertek is either a trademark or registered trademark of Intertek Testing Services NA in the United States and/or other countries. USB-C is either a trademark or registered trademark of USB Implementers Forum, Inc. in the United States and/or other countries. Wi-Fi is either a trademark or registered trademark of Wi-Fi Alliance in the United States and/or other countries. Other trademarks, registered trademarks, and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Crestron disclaims any proprietary interest in the marks and names of others. Crestron is not responsible for errors in typography or photography.
©2023 Crestron Electronics, Inc.

Contents

Overview 5
Crestron Flex Pod Wireless Speaker and Microphone 5
Crestron Flex Hub Wireless Transceiver 5
Crestron Flex Pod Wireless Audio Kit with Hub and Pod 5
Features 6
UC-AUDIO-POD Features 6
UC-AUDIO-HUB Features 8
Specifications 9
UC-AUDIO-POD Specifications 9
UC-AUDIO-HUB Specifications 12
Installation 14
UC-AUDIO-POD Installation 14
In the Box 14
Install the Pod 15
Connections 15
UC-AUDIO-POD-TTMK Installation 16
Install the Pod using UC-AUDIO-POD-TTMK 16
UC-AUDIO-HUB Installation 20
In the Box 20
Install the Hub 20
Connections 22
Pairing 23
Pair the Pod to the Hub 23
Unpair the Pod from the Hub 25
Important points 25
LED Indicators and Buttons 26
UC-AUDIO-POD LED Indicators and Buttons 26
Pod LED Indicators 26
Pod Buttons 27
Volume Functions 28
Factory Restore 28
UC-AUDIO-HUB LED Indicators and Buttons 29
Hub LED Indicators 29
Hub Buttons 30
Factory Restore 30
Configuration 31
Web Configuration 31
Action 33

Status 38
Settings 41
Security 51
802.1x Configuration 59
XiO Cloud Service 61
Crestron Settings App 62

Resources 64

Crestron Support and Training 64
Programmer and Developer Resources 64
Related Documentation 64

Overview

The Crestron Flex UC-AUDIO-POD and UC-AUDIO-HUB are wireless conferencing devices that provide a small to large room audio conference solution. The pod wirelessly connects to the hub through Digital Enhanced Cordless Telecommunications (DECT™) technology. Up to four pods can be connected to the hub, providing omnidirectional sound in small to large conference rooms and multi-purpose meeting spaces. See below the frequency range for your region.

Frequency Range	Countries
DR1: 1920 - 1930 MHz 5 channels	US and Canada
DR2: 1880 - 1900 MHz 10 channels	Europe, Australia, New Zealand, Israel, Saudi Arabia, Kuwait, Qatar, United Arab Emirates, Yemen, Oman, Hong Kong, Singapore and Iraq

NOTE: For simplicity within this documentation, the term "pod" is used for the UC-AUDIO-POD and "hub" is used for the UC-AUDIO-HUB, except noted otherwise.

The information provided in this product manual is applicable to the following pod and hub variants:

Crestron Flex Pod Wireless Speaker and Microphone

The Crestron Flex pod variants listed below are functionally similar.

- UC-AUDIO-POD-B-DR1
- UC-AUDIO-POD-B-DR2

Crestron Flex Hub Wireless Transceiver

The Crestron Flex hub variants listed below are functionally similar.

- UC-AUDIO-HUB-DR1
- UC-AUDIO-HUB-DR2

Crestron Flex Pod Wireless Audio Kit with Hub and Pod

The Crestron Flex pod wireless audio kit variants listed below are functionally similar.

- UC-AUDIO-1-B-DR1 KIT
- UC-AUDIO-1-B-DR2 KIT

Features

This section provides the following information:

- UC-AUDIO-POD Features
- UC-AUDIO-HUB Features

UC-AUDIO-POD Features

The Crestron Flex UC-AUDIO-POD is a wireless tabletop conferencing device with a speaker and four microphones that is ideal for small to large rooms. The pod wirelessly connects and transfers audio to and from a paired Crestron Flex UC-AUDIO-HUB. The connected hub receives and sends audio to a UC Engine through a USB-C® connection. Up to four pods can connect with the hub, providing omnidirectional sound in small to large conference rooms and multi-purpose meeting spaces. The pod can be placed anywhere within a room or mounted on a table, depending upon the size and shape of the meeting space.

A mic mute and unmute button, speaker volume indicator, and LED indicator ring display the pod's operational status. The volume levels are synchronized across all the pods in a conference room, maintaining audio level consistency. The pod is powered with a USB-C cable, connected to the supplied universal power adapter.



Key features include:

- A tabletop conferencing device with speaker and microphones for small to large rooms
- Wireless connectivity enables placement of the pod anywhere on a conference table
- Convenient in-call volume and mic mute controls
- Speaker volume indicator and LED indicator ring display the operational status

- Optional tabletop mounting accessory and Kensington® lock support
- Built-in AEC and noise reduction affords exceptional full-duplex audio performance with highly intelligible, echo-free two-way voice quality
- Up to four pods connect wirelessly to the hub which sends and receives audio to a UC Engine through USB connection
- DECT™ technology ensures minimal interference and robust security

High-Quality Audio

The pod delivers intelligible and high-quality audio across every corner of a room. It contains four auto-mixed directional mics that provide 360-degree pickup, high-quality echo cancellation, automatic gain compensation, and noise reduction.

Outstanding Adaptability

The pod is scalable across a variety of room types, including unconventionally shaped ones and those with challenging designs. In an open architecture design or where walls and ceilings cannot be opened to wires, the pod provides an audio solution ensuring that neither room aesthetics nor optimal audio are compromised. The pod, when connected with the hub, can easily be moved if furniture changes, and additional pods can be added if the room expands. Pods can be deployed in spaces with video conferencing hosted by personal devices to enable productive hybrid meetings with high-quality audio.

Plug-and-Play USB Connectivity

The pod turns on automatically when connected to the hub that is connected to a UC Engine through plug-and-play USB.

Robust Security

The pod delivers audio over long distances, making it optimal for larger spaces. The Digital Enhanced Cordless Telecommunications (DECT™) technology ensures that only paired pods transmit audio from the intended hub. The pod provides safe and secure audio transmission leveraging DECT technology. DECT uses multiple levels of security and does not interfere with other wireless technologies, such as Wi-Fi® and Bluetooth®.

Easy Device Management

The configuration and connection status of the pod can be monitored through a simple web user interface with no prior setup. Deploying pods across multiple room types, firmware updates, monitoring, and management can be controlled using the XiO Cloud® service.

UC-AUDIO-HUB Features

The Crestron Flex UC-AUDIO-HUB is a wireless transceiver and auto mixer that connects with up to four paired Crestron Flex UC-AUDIO-POD devices through Digital Enhanced Cordless Telecommunications (DECT™) technology. The hub receives audio from the pods' microphones, auto-mixes the audio, and transfers it to a UC Engine through a USB-C connection. The hub also distributes audio to all paired pods after receiving the audio from the UC Engine.



Key features include:

- A wireless transceiver and auto mixer for Crestron Flex Pods
- Pairs with up to four pods via DECT™ technology
- DECT technology ensures minimal interference and robust security
- Connects to a UC Engine through a USB-C cable, transferring auto-mixed audio to the UC Engine

Wireless Connectivity

The hub wirelessly connects with and distributes audio to up to four paired pods, enabling the pods to be placed anywhere within a room. This allows the hub and the pods to be deployed in large conference rooms and multi-purpose meeting spaces. Audio level consistency is realized as volume levels are synchronized across all the pods.

Robust Security

The hub provides safe and secure audio transmission to and from the pods by leveraging DECT technology. DECT uses multiple levels of security and does not interfere with other wireless technologies, such as Wi-Fi® and Bluetooth®.

Easy Device Management

The configuration and connection status of the hub can be monitored through a simple web user interface with no prior setup. Firmware updates, monitoring, and management can be controlled using the XiO Cloud® service.

Specifications

This section provides the following information:

- UC-AUDIO-POD Specifications
- UC-AUDIO-HUB Specifications

UC-AUDIO-POD Specifications

Speaker

Driver	One full range 2 in. speaker
Frequency Response	100 Hz to 7 kHz
Output Level	74 dB SPL at 1 m

Microphones

Microphones	360° quad mic array
Pickup Range	7.5 ft (approx. 2.3 m)

Audio

DSP	Acoustic echo cancellation, automatic gain control, dynamic noise suppression, and speaker volume control Full-duplex IEEE 1329 Type 1 compliant

Wireless Communication

Frequency	Frequency bands: **DR1:** 1920 – 1930 MHz 5 channels (For US and Canada only) **DR2:** 1880 – 1900 MHz 10 channels (For Europe, Australia, New Zealand, Israel, Saudi Arabia, Kuwait, Qatar, United Arab Emirates, Yemen, Oman, Hong Kong, Singapore and Iraq) Range up to 50 ft (approx. 15 m) indoors

Indicators

Mic Unmute	Green LED indicates microphone is unmuted
Mic Mute	Red LED indicates microphone is muted
Volume Level	White LED indicates the speaker volume

Buttons

Speaker Volume Up / Down	Capacitive, backlit
Mic Mute	Capacitive, backlit

Pair	Push button
Reset	Recessed push button

Connectors

USB-C	5VDC, 3A via external 100-240VAC power pack (included with the pod)
Security Port	Kensington Security Slot™ port

Environmental

Temperature	41° to 104° F (5° to 40° C)
Humidity	10% to 95% RH (non-condensing)
Heat Dissipation	12 BTU/hr

Construction

Enclosure	Lightly textured black/white finish, plastic housing, perforated stainless steel grilles, and die-cast aluminum bottom cover
Mounting	Tabletop mounting only

Dimensions

Height	3.0 in. (76 mm)
Width	4.40 in. (112 mm)
Depth	4.40 in. (112 mm)

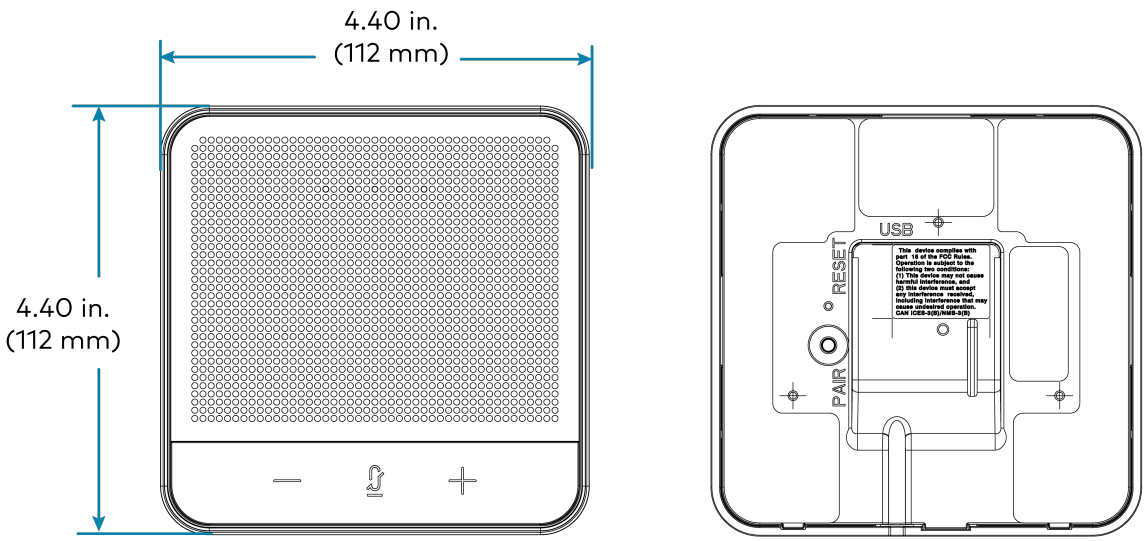
Weight

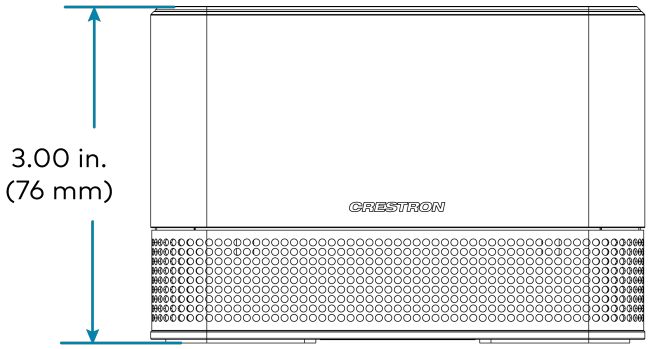
1.6 lb (726 g)

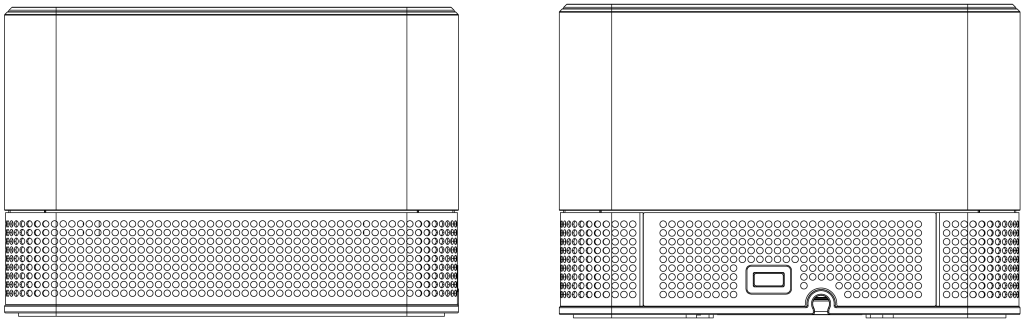
Compliance

Regulatory Model: M202109002
IC, CE, FCC Part 15 Class B digital device, Intertek® Listed for US & Canada

Dimension Drawings







UC-AUDIO-HUB Specifications

Wireless Communication

Frequency	Frequency bands: **DR1:** 1920 – 1930 MHz 5 channels (For US and Canada only) **DR2:** 1880 – 1900 MHz 10 channels (For Europe, Australia, New Zealand, Israel, Saudi Arabia, Kuwait, Qatar, United Arab Emirates, Yemen, Oman, Hong Kong, Singapore and Iraq) Range up to 50 ft (approx. 15 m) indoors

Indicators

Power	Green LED indicates the power is on
Sync	Five SYNC LEDs indicate pairing and connection with each pod[1]

Buttons

Pair	Tactile push button
Reset	Recessed push button

Connectors

USB-C	USB-C (PC) Connection for Audio and HID data
24VDC, 0.75A	24VDC, 0.74A via external 100-240VAC power pack, (included with the hub)
RJ-45	1000 Mbps Ethernet

Environmental

Temperature	41° to 104° F (5° to 40° C)
Humidity	10% to 95% RH (non-condensing)
Heat Dissipation	12.3 BTU/hr

Construction

Enclosure	Lightly textured black finish, plastic housing
Mounting	Freestanding, stackable, surface mount and wall/ceiling mount option with bracket (black plastic)

Dimensions

Height	1.35 in. (34 mm), 1.77 in. (45 mm) with bracket
Width	5.04 in. (128 mm), 5.36 in. (137 mm) with bracket
Depth	5.04 in. (128 mm)

Weight

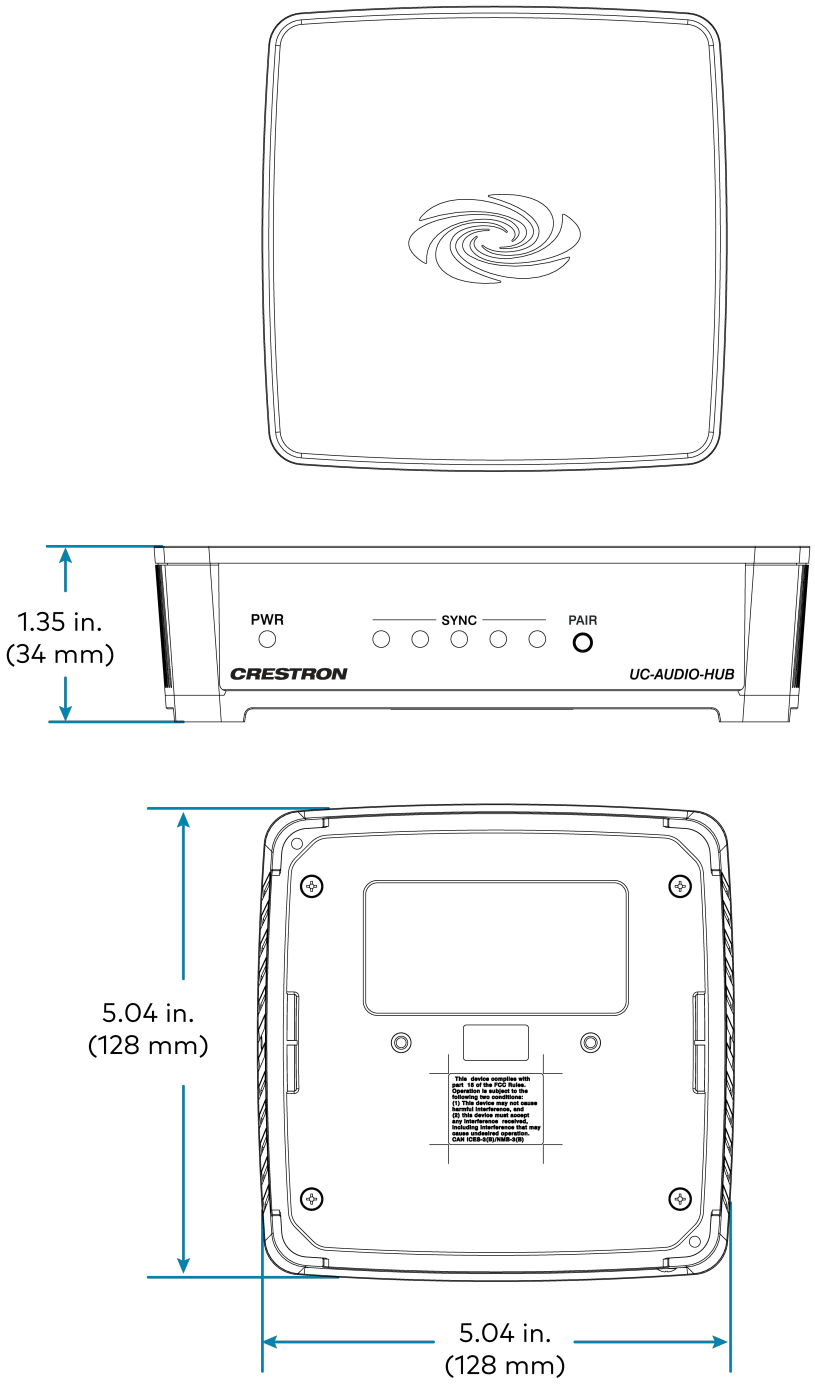
8.9 oz (253 g) without bracket

Compliance

Regulatory Model: M202109001

IC, CE, FCC Part 15 Class B digital device, Intertek® Listed for US & Canada

Dimension Drawings



Installation

This section provides the following information:

- UC-AUDIO-POD Installation
- UC-AUDIO-POD-TTMK Installation
- UC-AUDIO-HUB Installation
- Pairing

UC-AUDIO-POD Installation

Refer to the following for instructions on how to install the pod:

In the Box

Qty.	Description
1	UC-AUDIO-POD, Crestron Flex Pod Wireless Speaker and Microphone
	Additional Items
1	PWR Pack, 5VDC, 3A, 100-240VAC IN, USB-C Connector (2059526)
1	Bracket, Steel (2059413)
1	Screw, 04-40, 3/16 in., Pan Head, Steel (2007148)

Install the Pod

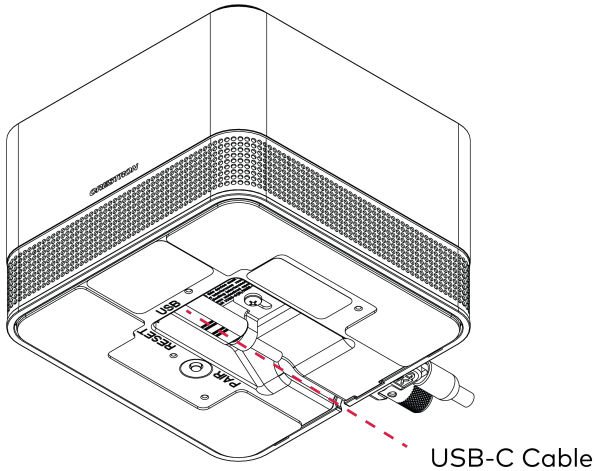
The UC-AUDIO-POD can be placed on any flat surface or secured on a table using the UC-AUDIO-POD-TTMK tabletop mounting kit (sold separately).

Refer to UC-AUDIO-POD-TTMK Installation on page 16 to install the pod with the tabletop mounting kit.

Connections

Connect the included USB-C cable to the **USB** port at the bottom of the pod to supply power from the included power adapter.

> **NOTE:** Use the supplied USB-C cable to supply power from the included power adapter. Power from other USB-C based power sources may lead to inconsistent operation and audio drop-out.



UC-AUDIO-POD-TTMK Installation

Refer to the following for instructions on how to install the tabletop mounting kit:

In the Box

Qty.	Description
1	UC-AUDIO-POD-TTMK, Tabletop Mounting Kit for Crestron Flex Pod Wireless Speaker and Microphone
	Additional Items
1	Cable Organizer (4534845)
1	Table Mount, Plastic (2060074)
3	Screw, 02-56 X 3/16 in., Flat Head, Steel (2046401)

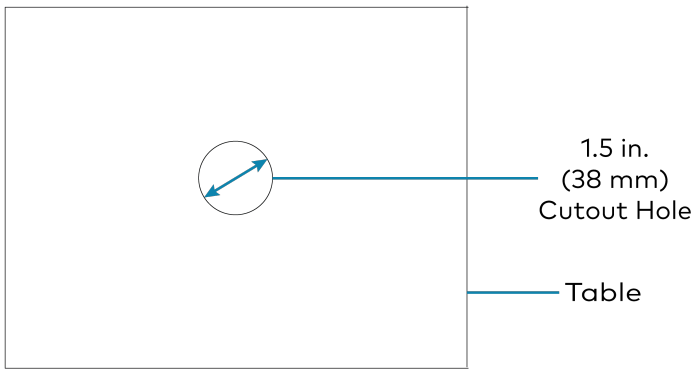
Install the Pod using UC-AUDIO-POD-TTMK

The UC-AUDIO-POD-TTMK is an optional mounting kit for the pod. The easy-to-install kit includes a plastic flange, threaded tube and two nuts to mount the pod on a table. An adhesive strip is attached to the bottom of the flange to prevent the pod from rotating on the table.

To install the UC-AUDIO-POD-TTMK on a table:

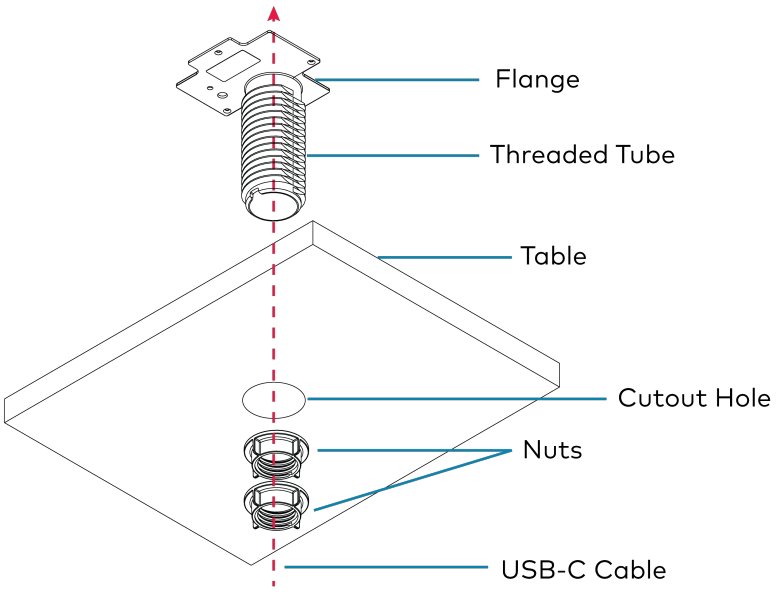
Prepare the Mounting Surface

- The mounting surface of the table must have a minimum thickness of 3/4 in. (19 mm) and a maximum thickness of 1.50 in. (38 mm).
- Cut a 1.50 in. (38 mm) wide hole in the table.

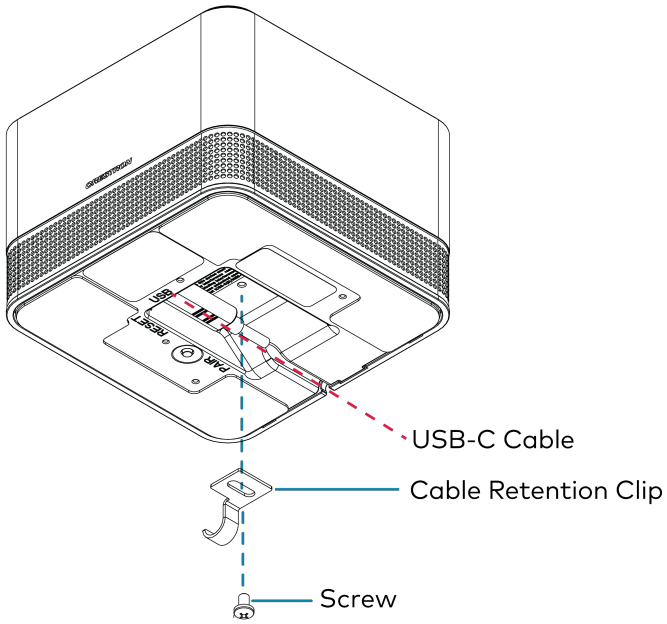


Attach the Mounting Kit

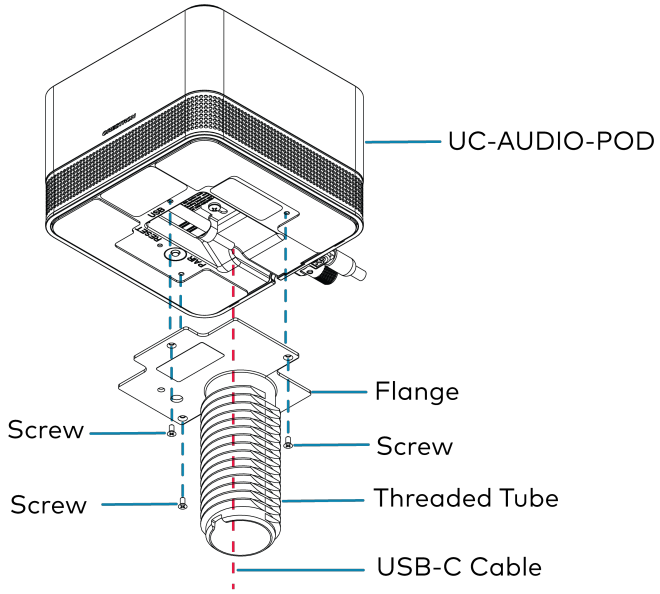
1. Route the USB-C cable first through the two nuts, then through the cutout hole in table, and finally into the mounting kit's threaded tube.



2. Connect the USB-C cable to the **USB** port at the bottom of the pod.
3. Secure the cable by attaching the cable retention clip with a 04-40, 3/16 in. screw.



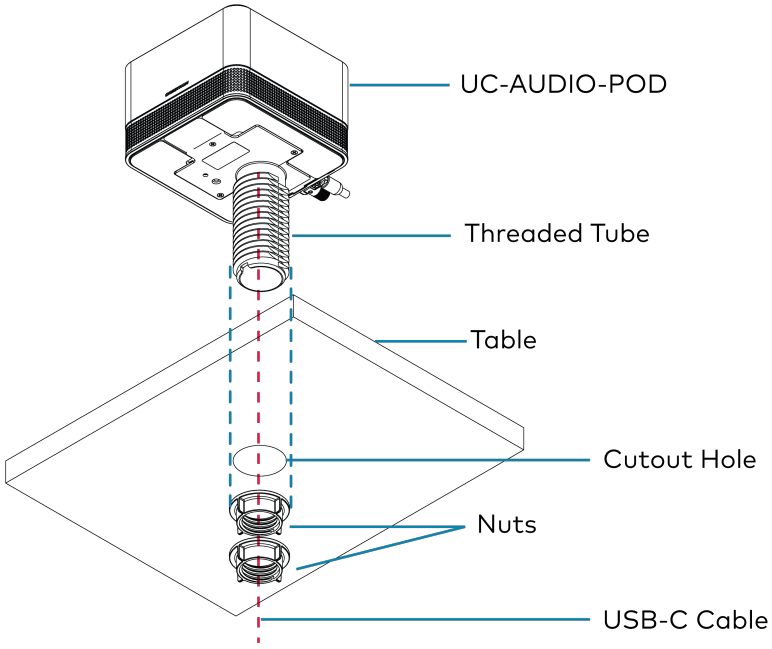
4. Attach the kit's flange to the bottom of the pod with the three 02-56 X 3/16 in. screws.



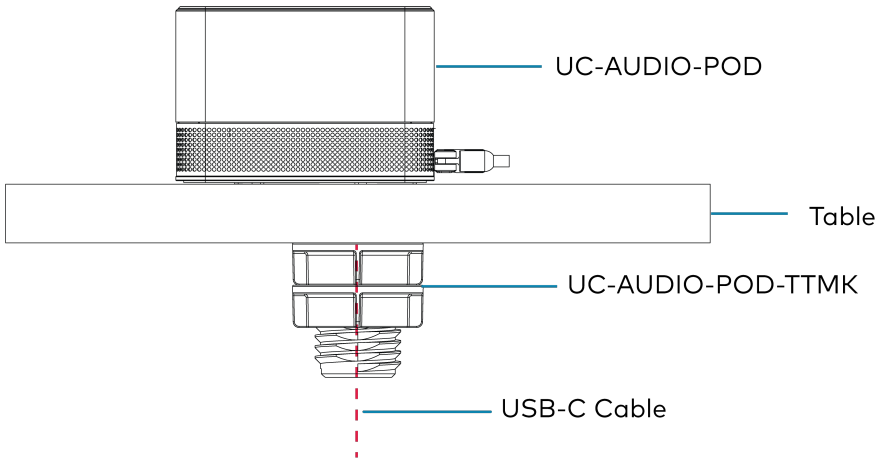
5. Peel off the adhesive strip attached to the bottom of the flange.

> **NOTE:** Peeling off the adhesive strip is optional. This ensures the pod remains tightened and cannot be rotated when mounted on the table.

6. Slide the kit's threaded tube into the cutout hole of the table.



7. Tighten and adjust the threaded tube with one nut first to achieve the desired resistance against the tube's motion.
8. Tighten the other nut to prevent the upper nut from slipping.



UC-AUDIO-HUB Installation

Refer to the following for instructions on how to install the hub:

In the Box

Qty.	Description
1	UC-AUDIO-HUB, Crestron Flex Hub Wireless Transceiver
	Additional Items
1	MTG Bracket with rail clip, plastic (4519035)
2	Screw, 06-32, 3/8 in., (2007225)
1	PWR Pack, 24VDC 0.75A, 100~240VAC IN, (2045865)

Install the Hub

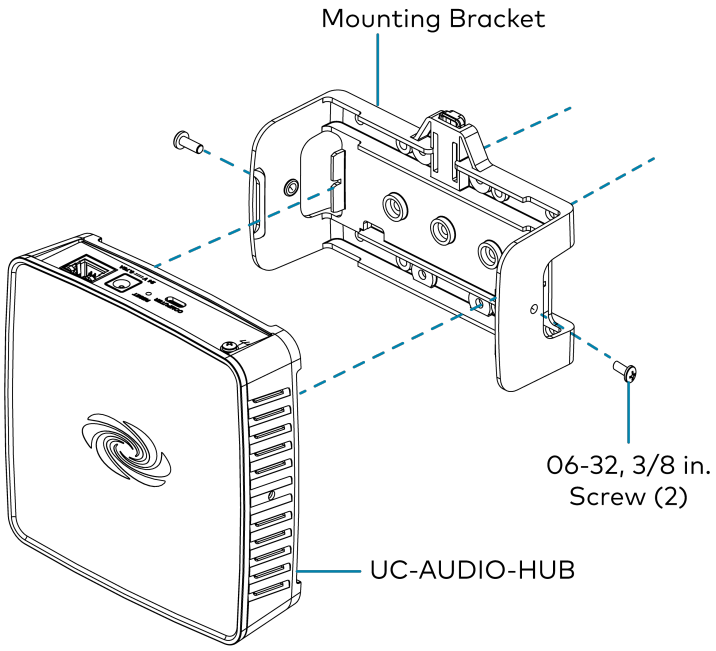
The hub can be mounted on a wall, DIN rail, or placed on any flat surface.

NOTES:

- Install the hub in a location that will provide optimum wireless performance.
- If the hub is installed behind a display, place it near an edge of the display to achieve the optimum wireless performance.
- It must be installed and used in accordance with appropriate electrical codes and regulations.

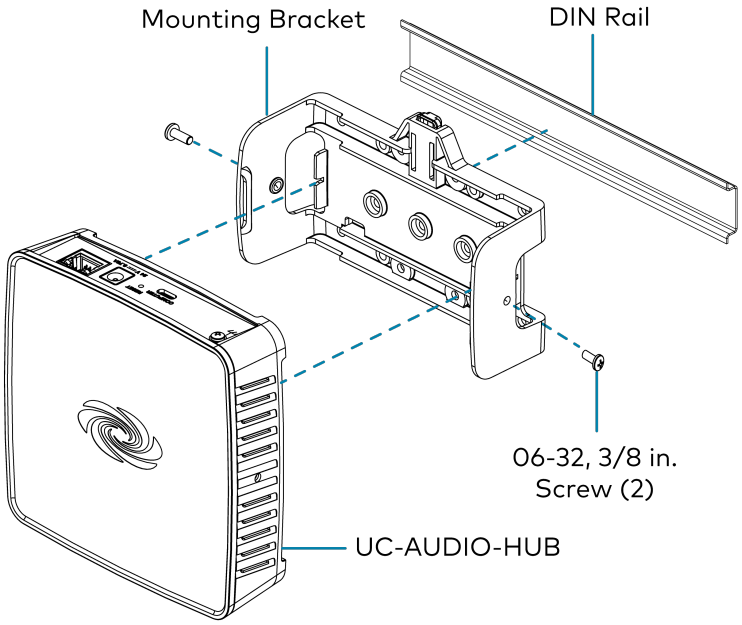
Wall Mount

1. Secure the mounting bracket to a vertical flat surface using screws that are appropriate for the mounting surface (not included).
2. Insert the hub into the mounting bracket until it snaps into place.
3. Install a 6-32 x 3/8 in. screw to each side of the mounting bracket to secure the hub.



DIN Rail Mount

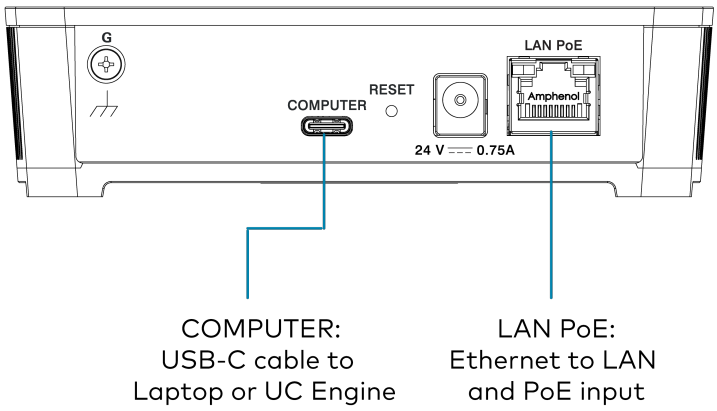
1. Hang the mounting bracket on the top of the DIN rail and press the top of the bracket toward the DIN rail until it snaps into place.
2. Insert the hub into the mounting bracket until it snaps into place.
3. Install a 6-32 x 3/8 in. screw to each side of the mounting bracket to secure the hub.



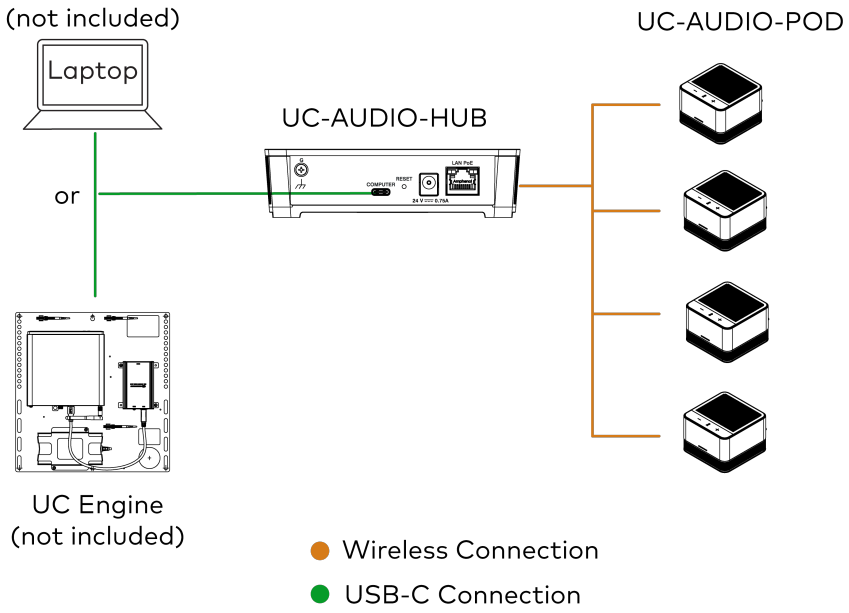
Connections

Make connections to the hub as shown in the following diagram:

> **NOTES:**
>
> - Use the **Computer** port to connect the USB-C cable to a laptop or UC Engine.
> - Use the **LAN PoE** port for Ethernet to LAN and PoE input.



Once the hub is connected to the laptop or UC Engine, pair the pod to the hub if it has not been paired before. For more information, refer to Pairing on page 23.



Pairing

Refer to the following points before pairing the pod to the hub:

- Up to four pods can be paired to the hub.
- The maximum distance between the pod and the hub is 50 ft (approx. 15 m) indoors.

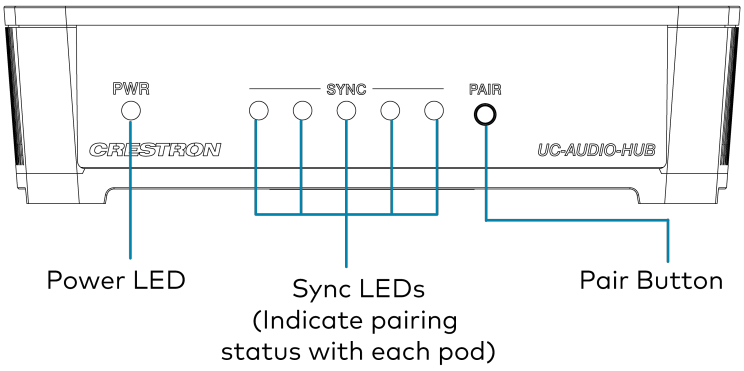
Pair the Pod to the Hub

To pair the pod with the hub:

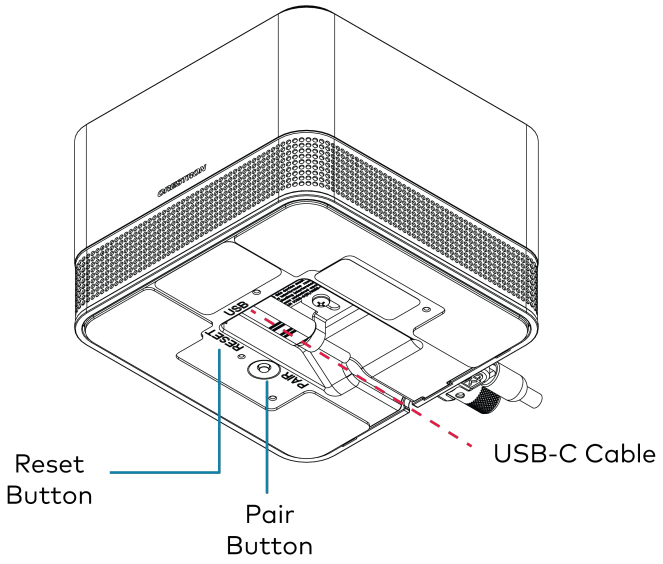
1. Press and hold the **PAIR** button on the hub for two seconds to enter the pair mode.

   NOTES:

   - The pod can only be paired manually to the hub. Pairing the pod is not possible in the web UI.
   - The hub can be paired manually or in the web UI. For more information, refer to Web Configuration on page 31.
   - The hub exits pair mode after two minutes of inactivity. The pod must be paired to the hub before the hub exits the pair mode.

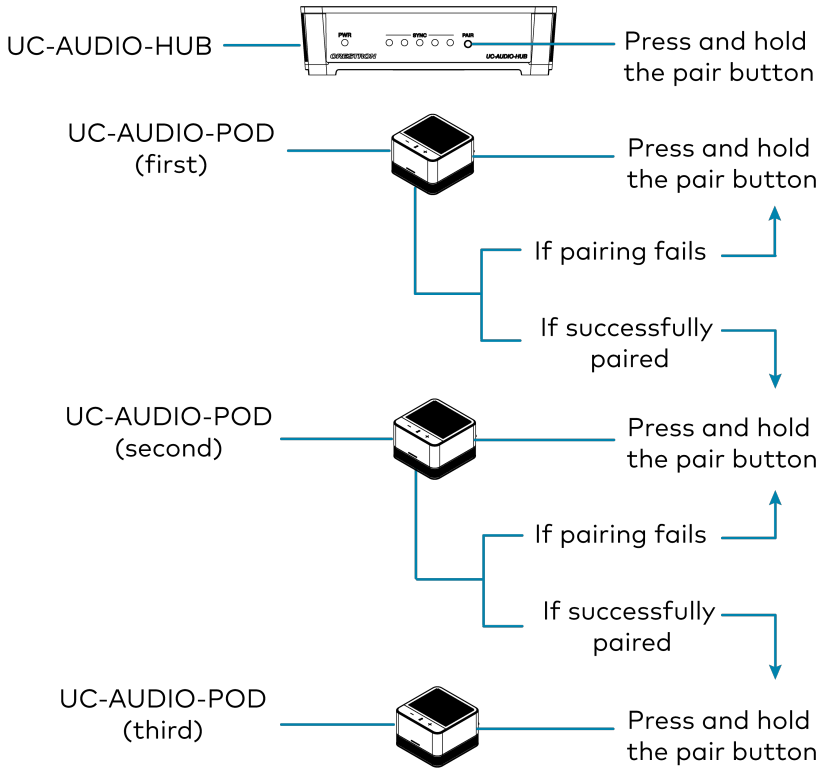


2. Press and hold the **PAIR** button at the bottom of the pod until the LED ring at the top blinks blue, then green twice quickly, and finally turns solid green indicating the pod is successfully paired to the hub. For more information, refer to Pod LED Indicators on page 26.



3. Once a pod is paired to the hub, follow the same procedure for the remaining pods.

> **NOTE:** Only one pod can be paired at a time. Wait until a pod's pairing is confirmed before pairing another one.



Follow the same procedure to pair the fourth pod.

Unpair the Pod from the Hub

1. Press and hold the **PAIR** button on the pod for ten seconds until the LED ring at the top blinks blue twice and then turns solid amber, indicating the pod has successfully been unpaired. Repeat the procedure for each pod you want to unpair.

   > **NOTE:** Unpairing the pod can also be done through the web UI. For more information, refer to Web Configuration on page 31.

2. Press and release the **PAIR** button on the hub to exit the pair mode.

Important points

- If the hub is factory restored, all the paired pods must be manually unpaired and then re-paired. For more information, refer to Factory Restore on page 28.
- For firmware updates, all pods should be kept in the same room with power on and within 50 ft (approx. 15m) of the paired hub.
- Pods are automatically updated by the paired hub after the hub receives a firmware update.

LED Indicators and Buttons

This section provides the following information:

- UC-AUDIO-POD LED Indicators and Buttons
- UC-AUDIO-HUB LED Indicators and Buttons

UC-AUDIO-POD LED Indicators and Buttons

Pod LED Indicators

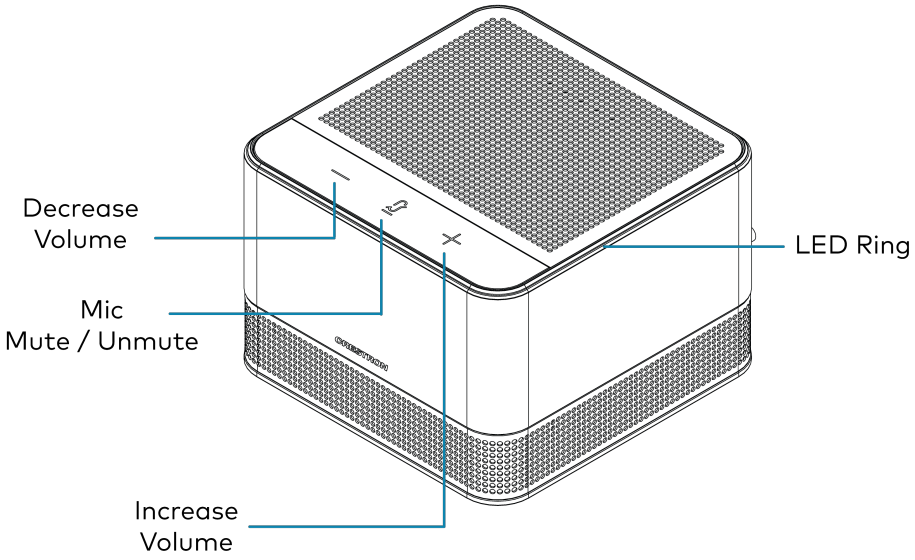
Refer to the following table for information about the pod LED indicators:

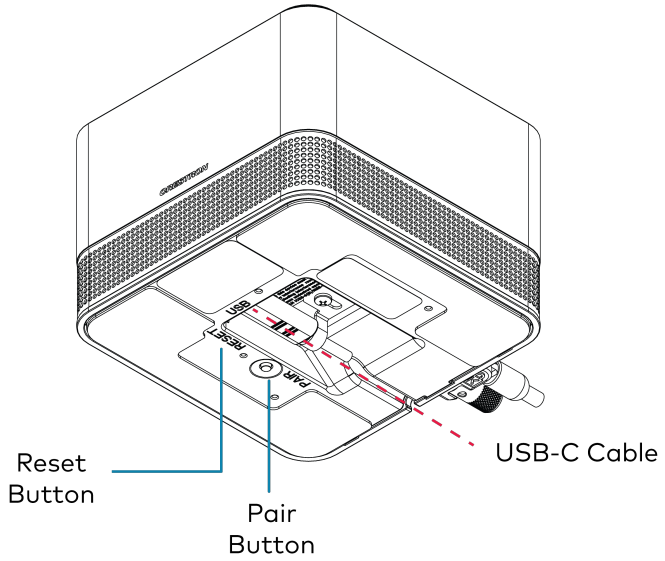
LED Indicator	Function	Color	Behavior	Indication
LED Ring	Mute Status	Red	Solid	The pod is paired to the hub and the mic is muted.
		Green	Solid	The pod is paired to the hub and the mic is unmuted.
	Pair	Amber	Solid	The pod is unpaired from the hub.
		Blue	Blinking (1/2s on, 1/2s off, 1/2s on, 1/2s off...)	The pod is actively getting paired to the hub.
	RF Signal Status	Amber	Blinking (1/2s on, 1/2s off, 1/2s on, 1/2s off...)	The pod was previously paired to the hub, the wireless signal is now lost.
	Fault State	Red	Blinking (1s on, 1s off, 1s on, 1s off...)	The pod is in a fault state.
	Firmware Status	Blue	Double-blink (1/8s on, 1/8s off, 1/8s on, 5/8s off)	The firmware is being updated.
	Locate Status	Blue	Blinks rapidly and continuously	The web UI sends a 'Locate' command. The LED keeps blinking until the locate command is turned off or RF signal is lost.
	Factory Restore	Blue	Blinks twice quickly	The pod factory restore is initiated.
Volume Bar	Volume Level	White	Solid	Current volume level is displayed.

Pod Buttons

Refer to the following table for the pod button functions:

Buttons	Functions
Volume Up (+)	Increases volume.
Volume Down (-)	Decreases volume.
Mic Mute/Unmute	Mute or unmute microphone.
Reset	Factory restore.
Pair	Pairs the pod to the hub.





Volume Functions

- There are five steps to adjust the pod's volume levels. Each of the five volume-level LEDs on the top of the pod represent a volume step. The white volume LEDs represent the current volume level.
- When a volume level is adjusted on one pod, the change automatically syncs across all other pods paired to the hub.
- When the + or - volume level button on the pod is pressed and held, the volume is increased or decreased until the button is released or the volume reaches the maximum or minimum level.
- A change in a pod's volume level automatically changes the UC Engine or laptop volume level.
- If the hub loses power or is rebooted, it will sync all pods to a default volume level once reconnected to the pods. Default volume level can be set from 0 to 100% through the web UI.
- If one or more pods are disconnected while the hub is powered on, the hub syncs the pods to the last volume level used when the pods are reconnected.

Group Mic Mute Functions

- A pod's microphone mute or unmute state is automatically synced across the other pods paired to the hub.
- The last mute or unmute setting used is retained once a pod's power cycle is completed.
- If one or more pods are disconnected while the hub is powered on, then the hub syncs the pods to the last mute or unmute state used when the pods are reconnected.
- When the hub completes its power cycle, all the paired pods are set to mute when reconnected to the hub.

Factory Restore

1. Press and hold the **RESET** button (using a paper clip) at the bottom of the pod for more than ten seconds to initiate a factory restore.
2. The LED ring blinks blue twice quickly, confirming the reset has initiated.

UC-AUDIO-HUB LED Indicators and Buttons

Hub LED Indicators

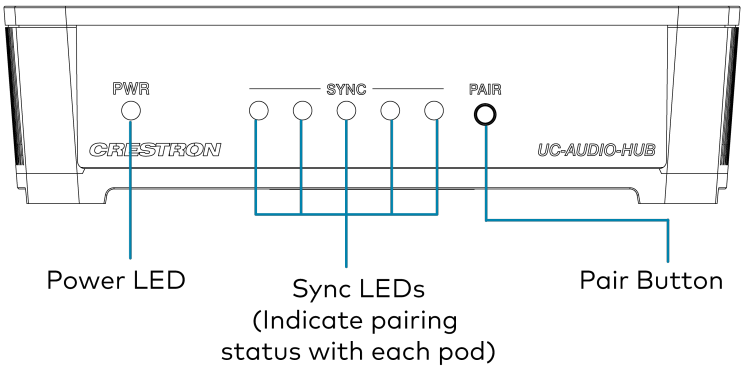
Refer to the following table for information about the hub LED indicators:

LED Indicator	Function	Color	Behavior	Indication
Power LED	Power Status	Green	Solid	The hub power is on and ready to use.
		Yellow	Solid	The hub power is on and not ready to use.
	DECT Firmware Status	Blue	Double-Blink (1/8s On, 1/8s Off, 1/8s On, 5/8 Off)	The DECT firmware update is in progress.
		Blue	Solid	The hub is in Bootloader mode.
	Fault State	Red	Solid	The hub is in a fault state.
	Factory Restore	Red	Blinks three times	The hub factory restore is initiated.
Sync LEDs	Pair	Blue	Dim	No pod is paired or connected.
		Green	Solid, Bright	Pod is paired, connected and is in an active audio call.
		Green	Dim	Pod is paired and connected, but not in an active audio call.
		Red	Blinking (1s on, 1s Off, 1s on, 2s Off ...)	Pod is paired and connected, but in a fault state.
		Amber	Blinking (1/2s On, 1/2s Off, 1/2s On, 1/2s Off...)	Pod is paired, but the signal is lost or out of range.
		Blue	Blinking (1/2s On, 1/2s Off, 1/2s On, 1/2s Off...)	Pod is not paired yet.
		Green	Blink twice quickly then change to solid	Pod is paired successfully.
		Red	Blink twice quickly then change to blinking blue (1/2s On, 1/2s Off...)	Pod pairing was unsuccessful.

Hub Buttons

Refer to the following table for the hub button functions:

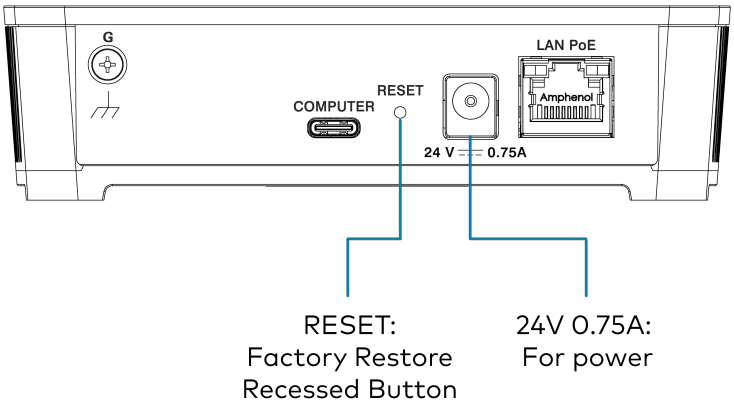
Buttons	Functions
Pair	Pairs the hub to the pod.
Reset	Factory restores the hub.



Factory Restore

1. Press and hold the **RESET** button (using a paper clip) on the back of the hub for more than 10 seconds to initiate a factory restore.
2. All LEDs on the front of the hub blink red three times, confirming the reset has initiated.

> **NOTE:** All pods should be factory restored before pairing again with a factory restored hub.



Configuration

Prior to configuration, ensure the hub is running the latest firmware. To update the firmware, refer to Update Firmware on page 34.

This section provides the following information:

- Web Configuration
- XiO Cloud Service
- Crestron Settings App

Web Configuration

The hub is configured using the web configuration interface. The configuration interface is accessible from a web browser once the hub's IP address is known.

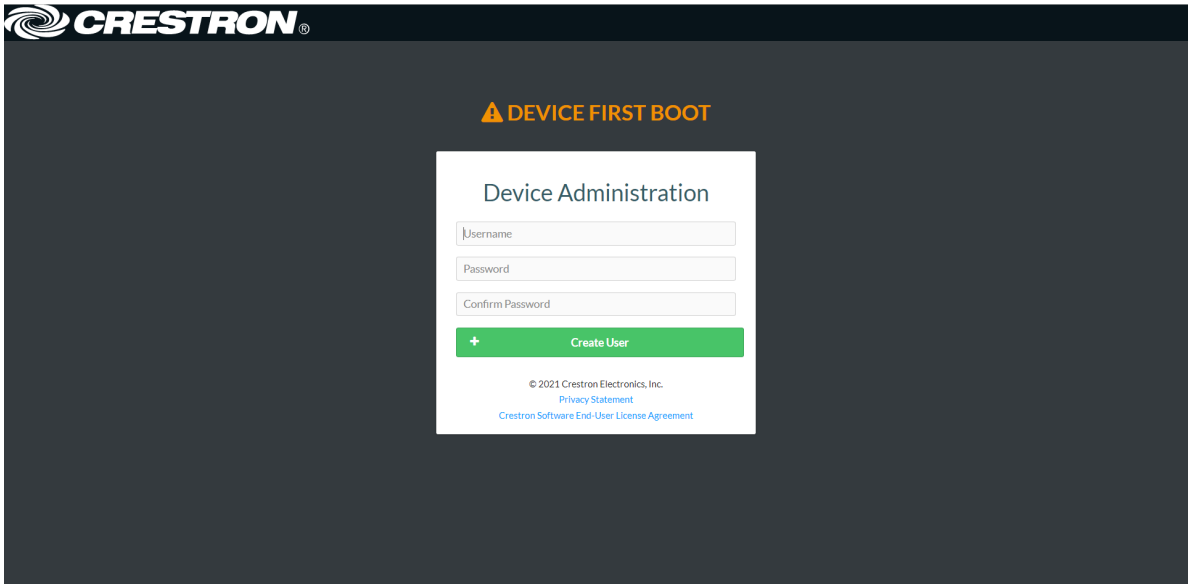
The web configuration interface is also accessible through the XiO Cloud Service on page 61 or Crestron Settings App on page 62.

> **NOTE:** The hub has to be connected with a network to access the web UI or XiO Cloud service.

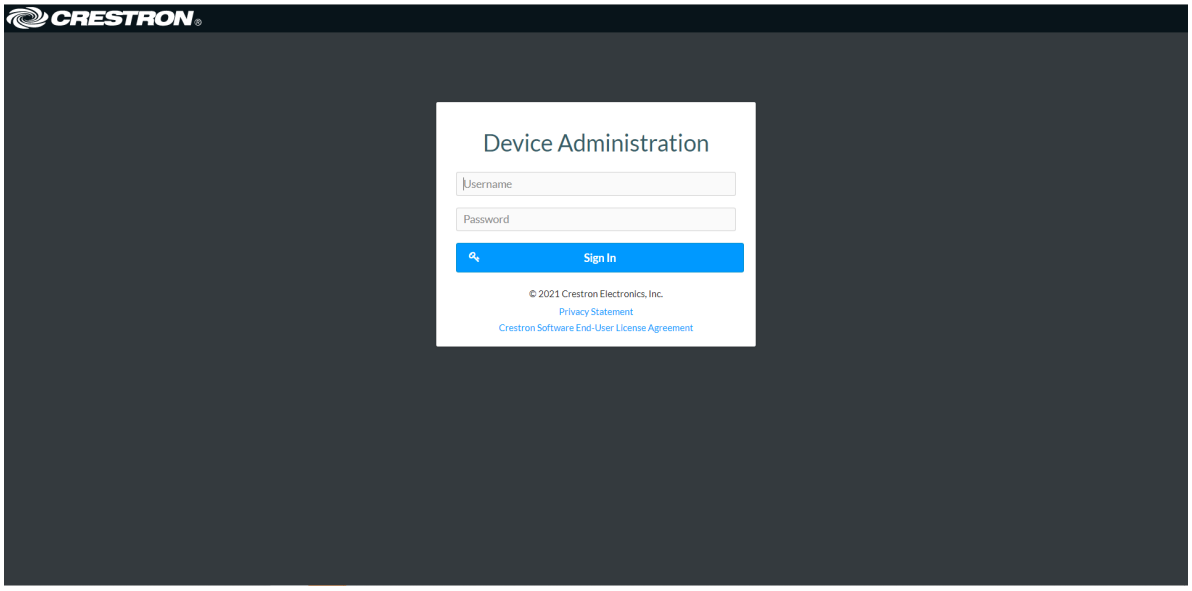
To access the web configuration interface:

1. Connect the hub to the same network as the host computer.
2. Use the **Device Discovery tool** in the Crestron Toolbox™ software to discover the hub and its IP address on the network.
3. Open a web browser.
4. Enter the hub IP address into the browser URL field.

5. If you are creating a user account for the first time, do the following; otherwise, skip to step 3.
   a. Enter a username in the **Username** field.
   b. Enter a password in the **Password** field. Re-enter the same password in the **Confirm Password** field.



   c. Click **Create User**. The Device Administration page appears.



6. Enter the username and password in their respective fields and select **Sign In** to continue. The web user interface is displayed.

Web User Interface



The web user interface displays the **Sign Out** button, **Action** drop-down menu and the following tabs:

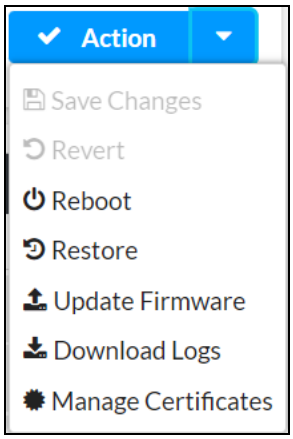
- **Status:** Used to monitor the hub status
- **Settings:** Used to configure the hub settings
- **Security:** Used to enable authentication and other security settings
- **802.1x Configuration:** Used to configure IEEE 802.1X network authentication for hub security

Action

The **Action** drop-down menu is displayed at the top right side of the interface and provides quick access to common hub functions, such as:

- Save Changes
- Revert
- Reboot
- Restore
- Update Firmware
- Download Logs
- Manage Certificates

Action Menu



Once any changes have been made to the hub configuration, the **Action** button changes to a **Save Changes** button. Select **Save Changes** to save changes to the configuration settings.

The **Action** menu provides the selections that follow.

Save Changes

Select **Save Changes** to save any changes made to the configuration settings.

Revert

Select **Revert** to revert the hub back to the last saved configuration settings.

Reboot

Select **Reboot** to restart the hub. After **Reboot** is selected, a dialog box is displayed asking whether the hub should be restarted. Select **Yes** to restart the hub or **No** to cancel the restart.

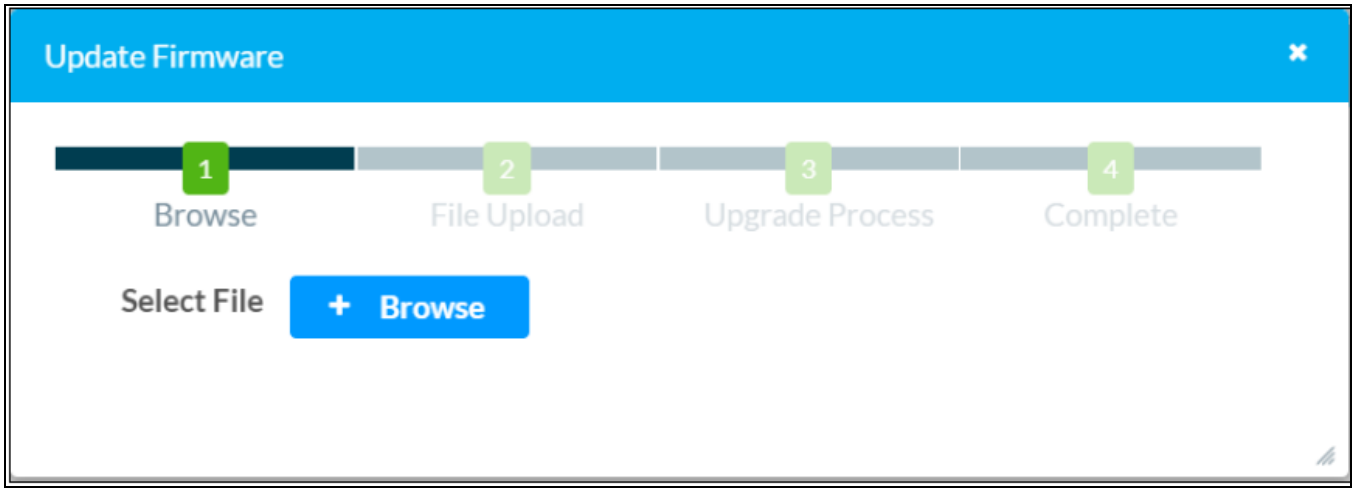
Restore

Select **Restore** to factory restore the hub configuration settings. After **Restore** is selected, a dialog box is displayed asking whether the hub settings should be restored to factory defaults. Select **Yes** to restore the settings or **No** to cancel the restore.

Update Firmware

Select **Update Firmware** to upgrade the hub's firmware manually with a downloaded PUF (package update file).

Update Firmware Dialog Box



To update the hub firmware PUF through the web user interface:

1. Visit the appropriate device product page or www.crestron.com/Support/Resource-Library to download the latest firmware PUF.
2. Select **Update Firmware**. The **Update Firmware** dialog box is displayed.
3. Select **Browse**, and then navigate to the firmware PUF on the host computer.
4. Select the firmware PUF, and then select **Open**.
5. Select **Load** to load the PUF to the hub. The upload progress is shown in the dialog box.
6. Once the hub has completed the firmware upgrade, select **OK**.

Select the **x** button to close the **Firmware Upgrade** dialog box at any time during the upgrade process. Selecting the **x** button before the PUF is uploaded to the hub cancels the upgrade.

NOTES:

- When the hub is connected to a UC Engine, firmware updates are performed through the UC Engine's Windows Update service.
- For time-based auto update of the firmware, refer to Auto Update on page 47.

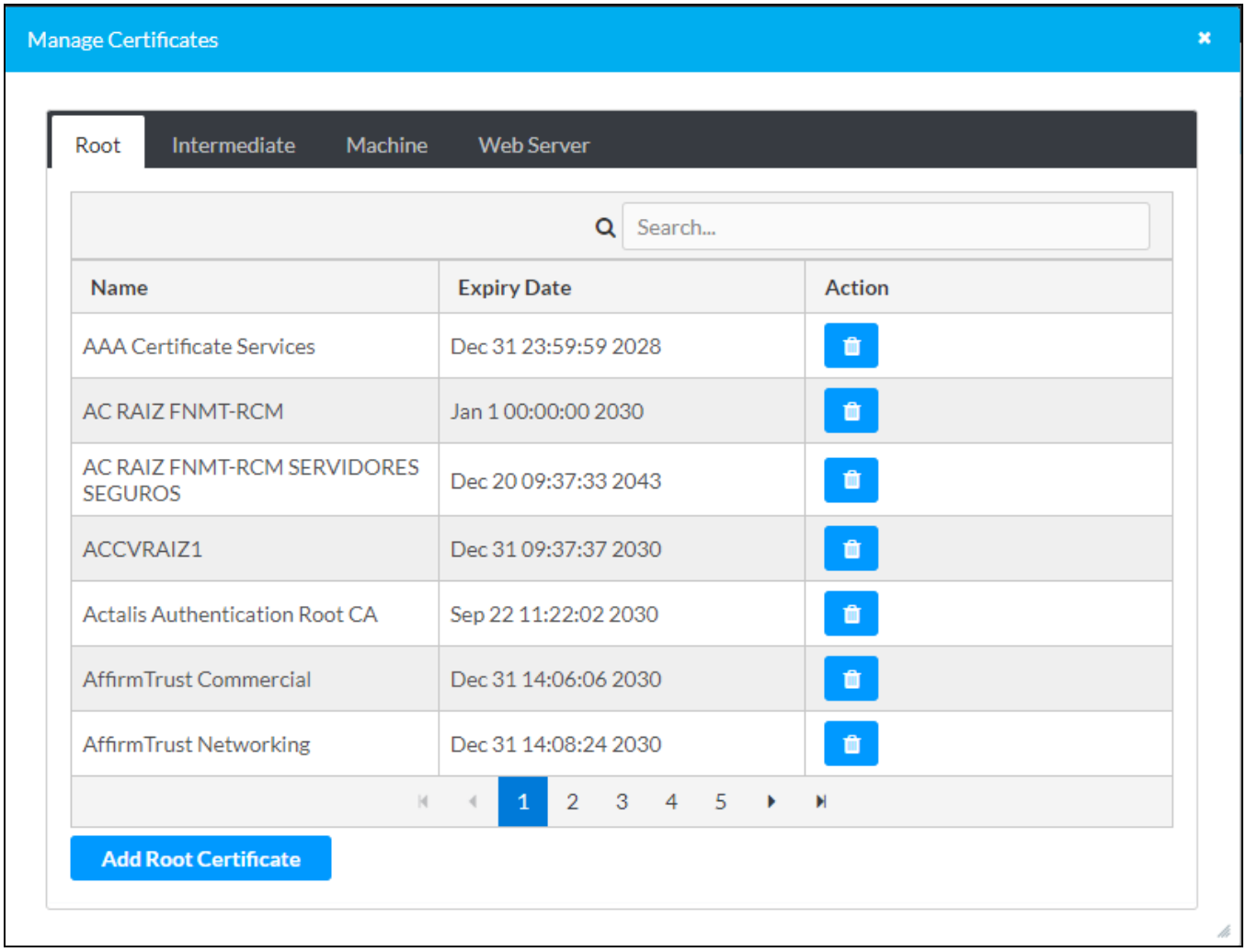
Download Logs

Select **Download Logs** to download the hub message logs for diagnostic purposes. The message files download as a compressed .tgz file. Once the compressed file is downloaded, extract the message log files to view them.

Manage Certificates

Select **Manage Certificates** to add, remove, and manage certificates used in 802.1x and other protected networks. The following certificate tabs are displayed:

Manage Certificates Dialog Box - Root Tab



- **Root:** The Root certificate is used to validate the network's authentication server. The hub has a variety of Root certificates, self-signed by trusted CAs (Certificate Authorities), and preloaded into the hub.
- **Intermediate:** The Intermediate certificates are non-self-signed certificates used to validate the authentication server. The network administrator will provide these certificates if the network does not use self-signed Root certificates.
- **Machine:** The Machine certificate is an encrypted PFX file that is used by the authentication server to validate the hub's identity. The Machine certificate will be provided by the network administrator, along with the certificate password.
- **Web Server:** The Web Server certificate is a digital file that contains information about the identity of the web server.

Search

Type a search term into the **Search...** text field to search for and display CAs that match the search term.

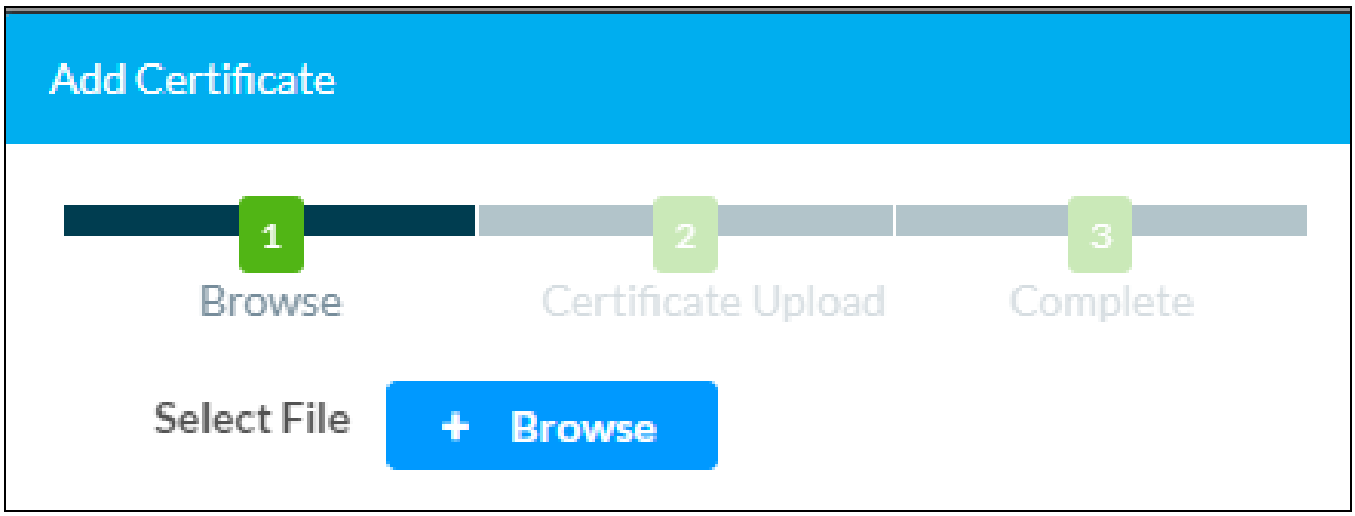
The following information is provided for each type of CA:

- **Name:** The CA name
- **Expiry Date:** The date and time that the CA is set to expire

If the CAs span multiple pages, use the navigation arrows on the bottom of the page to move forward or backward through the pages, or select a page number to navigate to that page.

Add Certificate

Add Certificate Dialog Box



1. Select **Add [Type] Certificate** to add a Certificate Authority (CA) of one of the four available types (**Root**, **Intermediate**, **Machine**, or **Web Server**) to the list of CAs. The **Add Certificate** pop-up dialog box is displayed.
2. Select the **+ Browse** button.
3. Navigate to the CA file on the host computer.
4. Select the CA file, and then click **Open**.
5. Select **Load** to load the CA file to the hub. The upload progress is shown in the dialog box.
6. Once the hub has completed the upload, click **OK**.

Delete Certificate

1. Select the corresponding certificate tab.
2. Select the trashcan button in the **Actions** column to delete the certificate. A pop-up dialog box is displayed asking if the CA should be deleted.
3. Select **Yes** to delete the certificate or **No** to cancel.

Status

The **Status** tab is the default tab that displays after login. The Status screen displays information about the hub and its other operating parameters.

Select a selection name to expand the selection. If the selection is expanded, select the selection name again to collapse the section.

Status Tab Selections

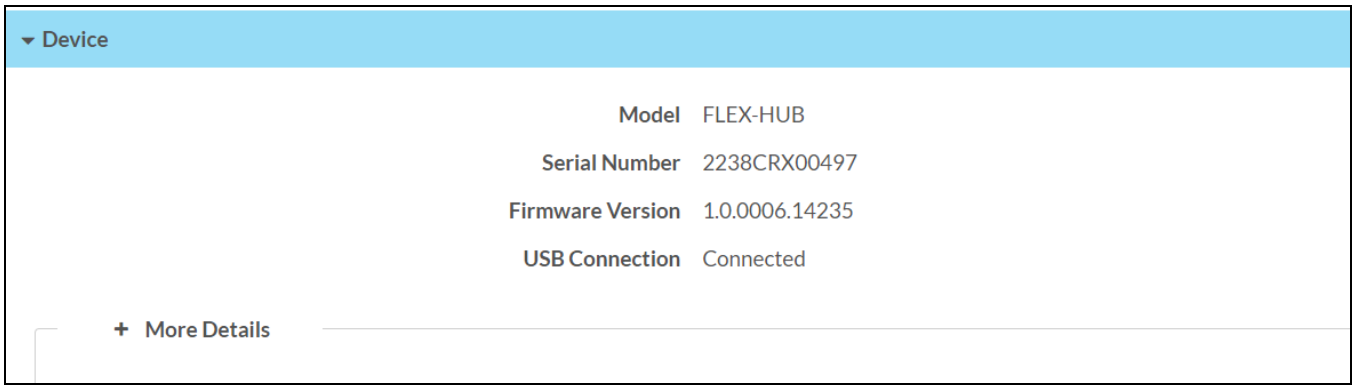


Each selection is described in the sections that follow.

Device

Select **Device** to view general device information.

Status Tab - Device



The following **Device** information is displayed:

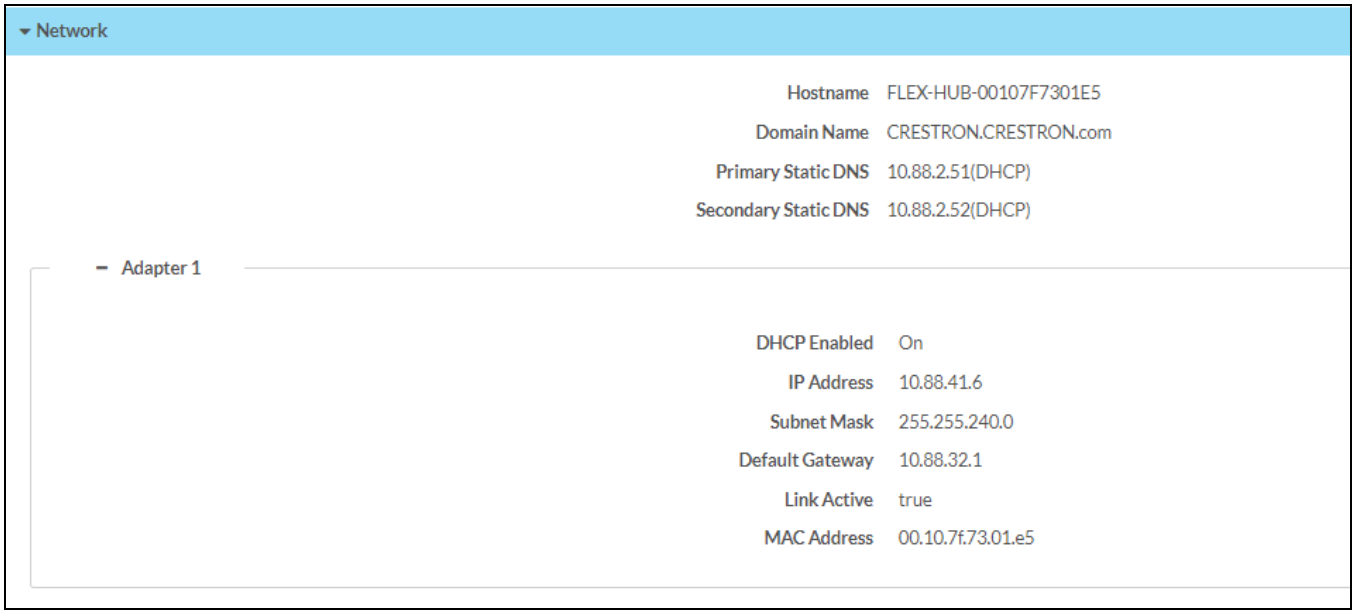
- **Model:** The hub model name
- **Serial Number:** The hub serial number
- **Firmware Version:** The firmware version loaded onto the hub
- **USB Connection:** Displays whether the USB is connected to a UC Engine or laptop

Select **+ More details** at the bottom of the **Device** tab to display an expanded section that shows additional hub information. If **+ More Details** is selected, select **- Less** details to collapse the section.

Network

Select **Network** to view the network settings status for the hub.

Status Tab - Network



The following **Network** information is displayed:

- **Hostname:** The hub hostname
- **Domain Name:** The hub domain name
- **Primary Static DNS:** The primary DNS (Domain Name Server) addresses used to resolve the hub domain to an IP address
- **Secondary Static DNS:** The secondary DNS (Domain Name Server) addresses used to resolve the hub domain to an IP address

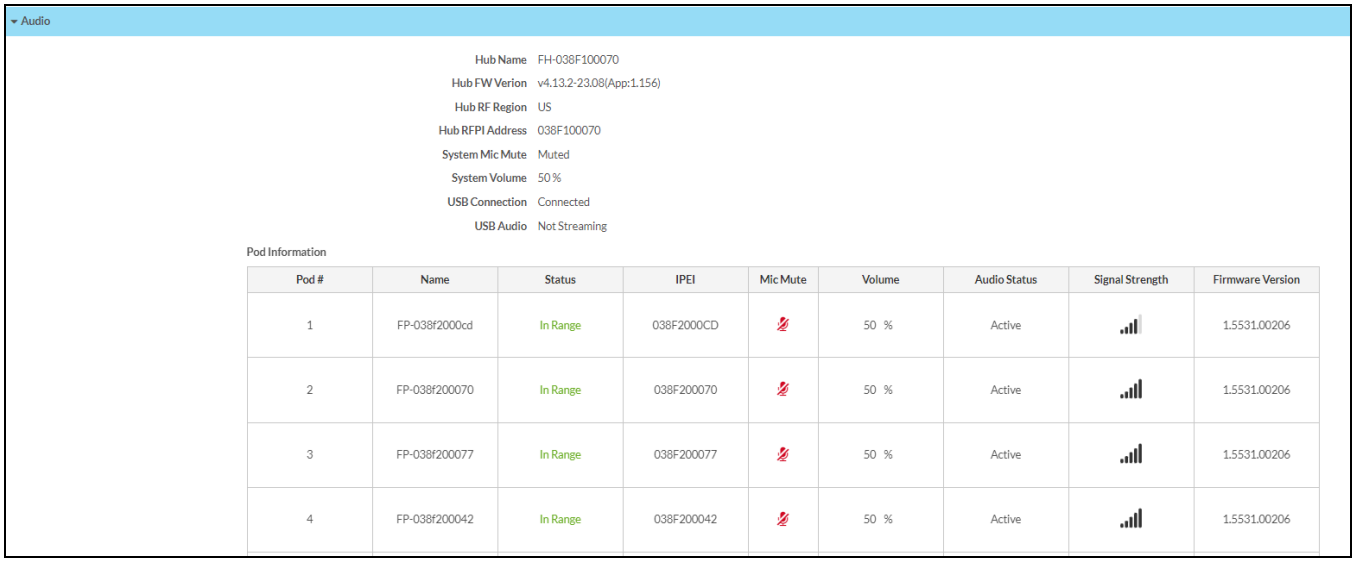
Select the **+** (plus) icon next to **Adapter 1** to display the following information:

- **DHCP Enabled:** Displays that DHCP (Dynamic Host Configuration Protocol) is selected for the hub IP address
- **IP Address:** The hub IP address, shown only if an Ethernet connection is active
- **Subnet Mask:** The hub subnet mask address, shown only if an Ethernet connection is active
- **Default Gateway:** The gateway router address, shown only if an Ethernet connection is active
- **Link Active:** Reports whether the Ethernet connection is active (true) or inactive (false)
- **MAC Address:** The unique hub MAC (media access control) address for the Ethernet adapter

Audio

Select **Audio** to view the audio status of the four pods paired to the hub.

Status Tab - Audio



The following **Audio** information is displayed:

- **Hub Name:** The hub name
- **Hub FW Version:** The hub firmware version
- **Hub RF Region:** The hub radio frequency region
- **Hub RFPI Address:** The hub Radio Fixed Part Identity address
- **System Mic Mute:** Status of the system mic
- **System Volume:** System volume level
- **USB Connection:** The hub USB connection status
- **USB Audio:** Displays if audio is being streamed between the hub and the laptop or the UC Engine

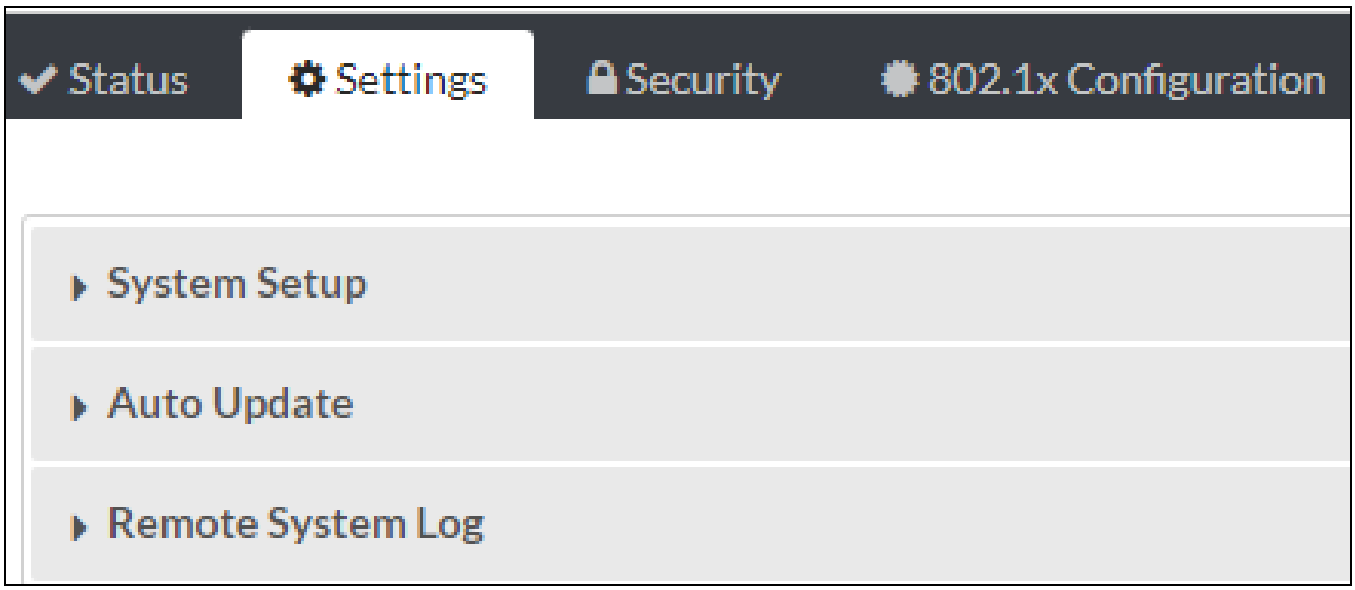
The following **Pod Information** table is displayed:

- **Pod#:** The pod number
- **Name:** An auto-generated pod name
- **Status:** Displays if the pod is within the hub's range or not
- **IPEI:** The pod unique identifier
- **Mic Mute:** Displays the pod mic mute status. If muted, it displays the microphone icon with a diagonally crossed sign in red color. If unmuted, the microphone color changes to green.
- **Volume:** The pod volume level
- **Audio Status:** Displays the pod audio status, either active or inactive
- **Signal Strength:** The pod radio frequency signal strength
- **Firmware Version:** The pod firmware version

Settings

Select the **Settings** tab on the top left of the interface to display selections for configuring various hub settings.

Settings Selections

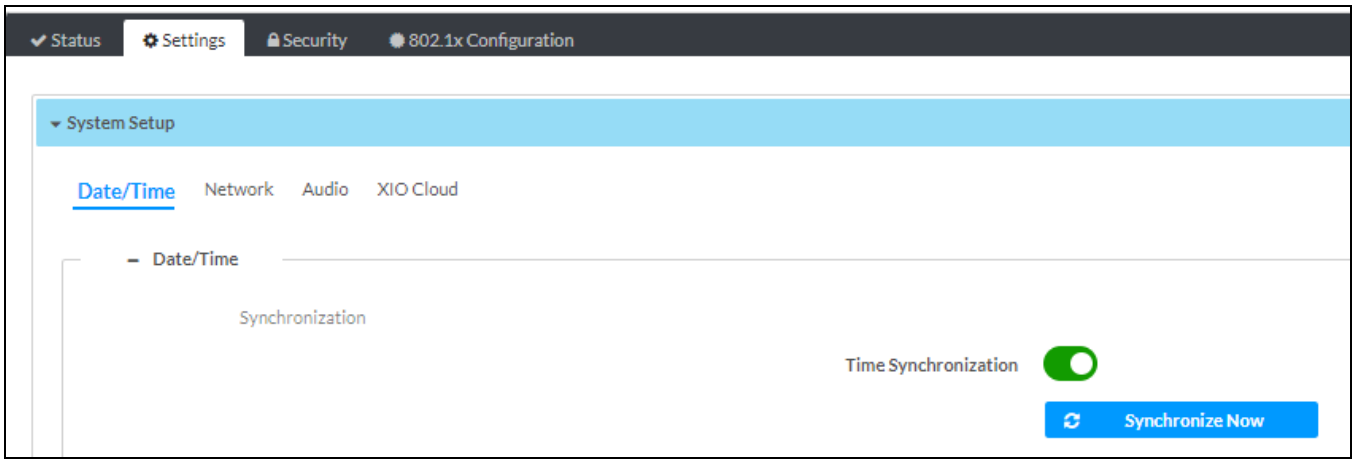


Each selection is described in the sections that follow.

System Setup

Select **System Setup** to configure date/time, network, audio and XiO Cloud settings.

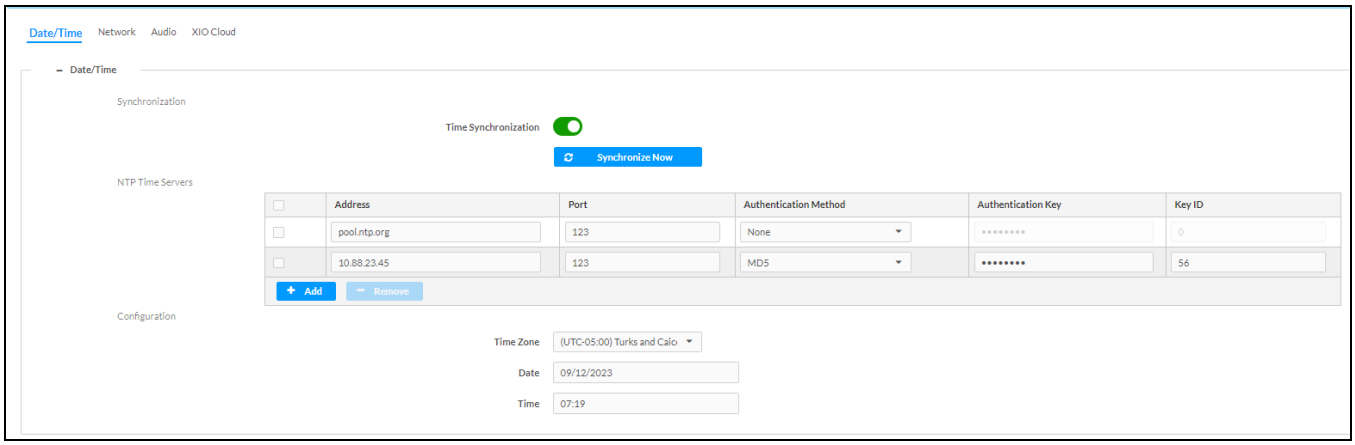
Settings Tab - System Setup



Date/Time

Select the **+** (plus) icon next to **Date/Time** to display the following date and time settings.

Settings Tab - System Setup (Date/Time)



Synchronization

- **Time Synchronization:** Slide the toggle to the right (enable) or left (disable) to specify time synchronization via SNTP (Simple Network Time Protocol). By default, time synchronization is enabled.
- **Synchronize Now:** With **Time Synchronization** enabled, select **Synchronize Now** to synchronize the hub with the SNTP server(s) entered in the **NTP Time Servers** table.
- **NTP Time Servers:** With **Time Synchronization** enabled, use the provided table to enter information regarding the SNTP server(s) used to synchronize the date and time for the hub.
    - Select **Add** to add a new SNTP server entry into the table.
    - Enter the following information for each entry:
        - Enter the SNTP server address into the **Address** text field.
        - Enter the SNTP server port into the **Port** text field.
        - Use the **Authentication Method** drop-down menu to select the authentication method used to access the SNTP server (if one exists).
        - If an authentication method is selected, enter the key used to authenticate against the SNTP server into the **Authentication Key** text field.
        - If an authentication method is selected, enter the ID for the key used to authenticate against the SNTP server into the **Key ID** text field.
    - To remove an entry, fill the check box to the left of the table entry, and then select **Remove**.

Time Configuration

- **Time Zone:** Select a time zone for the hub using the drop-down menu.
- **Date:** Select the date for the hub using the pop-up calendar that is displayed.
- **Time:** Enter the current time for the hub (in 24-hour format) using the pop-up menu that is displayed.

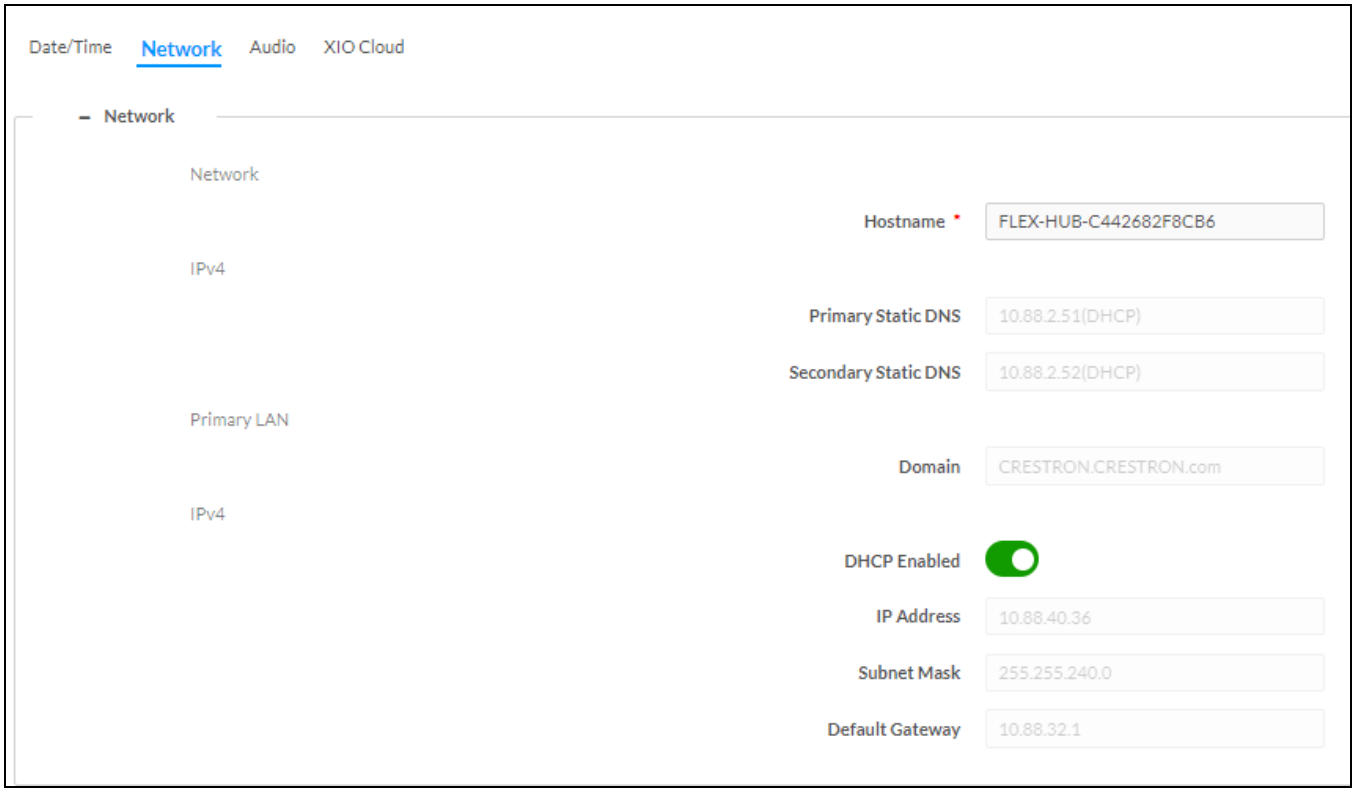
Select the **Save Changes** button displayed on the top right to save the settings.

Select **Revert** from the **Action** drop-down menu to revert to the previous settings without saving.

Network

Select the **+** (plus) icon next to **Network** to display the following network settings.

Settings Tab - System Setup (Network)



- **Hostname:** The hub hostname
- **IPv4:** The hub IP version
  - **Primary Static DNS:** The primary DNS (domain name server) address used to resolve the hub domain to a IPv4 address
  - **Secondary Static DNS:** The secondary DNS (domain name server) address used to resolve the hub domain to a IPv4 address
- **Primary LAN:** Displays the domain
  - **Domain Name:** Displays the domain name of the host

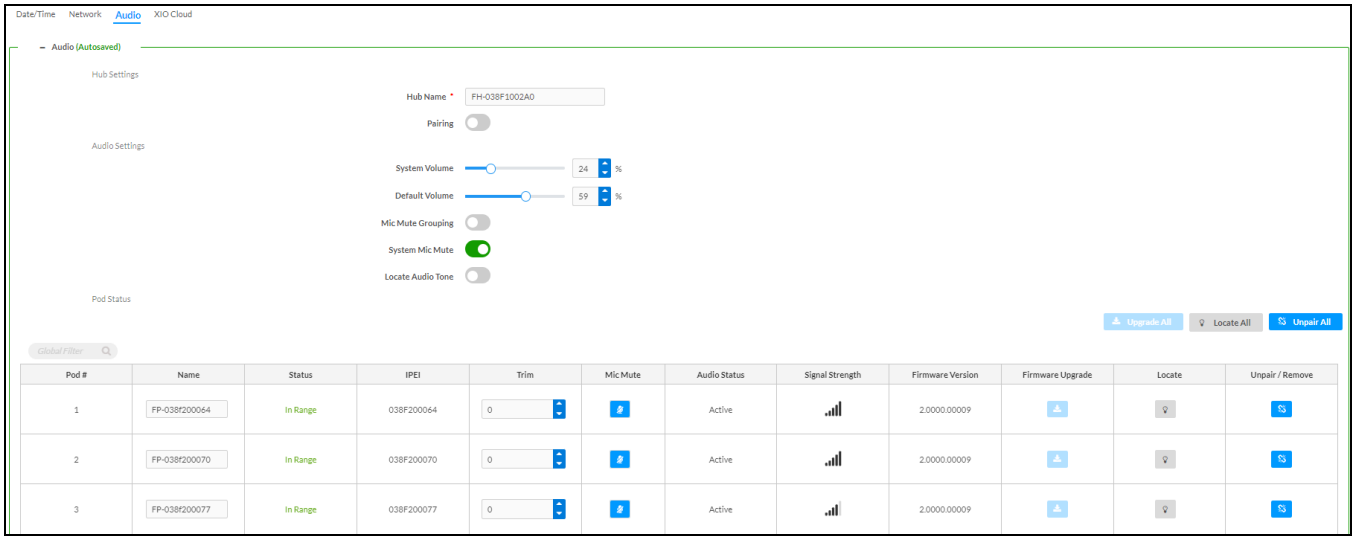
- **IPv4:** The hub IP version.
    - **DHCP Enabled:** Slide the toggle to the right (enable) or left (disable) specifying whether the hub's IP address is to be assigned by a DHCP server.
        - **Enabled:** When DHCP is enabled (default setting), the hub IP address is automatically assigned by a DHCP server on the local area network (LAN) for a predetermined period of time.
        - **Disabled:** When DHCP is disabled, manually enter information in the following fields:
            - **Primary Static DNS**: Enter a primary DNS IP address.
            - **Secondary Static DNS:** Enter a secondary DNS IP address.
            - **IP Address:** Enter a unique IP address for the hub.
            - **Subnet Mask:** Enter the subnet mask that is set on the network.
            - **Default Gateway:** Enter the IP address that is to be used as the network's gateway.
    - **IP Address:** The hub IP address
    - **Subnet Mask:** The hub subnet mask
    - **Default Gateway:** The gateway router address

Select the **Save Changes** button displayed on the top right to save the new network entries.

Audio

Select the **+** (plus) icon next to **Audio (Autosaved)** to display the following audio settings.

Settings Tab - System Setup (Audio)



- **Hub Settings:** The hub settings
  - **Hub Name:** The hub name
  - **Pairing:** Slide the toggle to the right to pair the hub with the pods. Pairing the hub with the pods can also be done manually.
- **Audio Settings:** The pod audio settings
  - **System Volume:** The system volume for the pods can be set from 0% to 100%. Increase or decrease the system volume using the upper and lower arrows. Any change done to the volume level will automatically sync across all other pods paired to the hub.
  - **Default Volume:** The default volume for all the pods can be set from 0% to 100%. Increase or decrease the default volume using the upper and lower arrows. If the hub loses power or is rebooted, the default volume level will sync across all the paired pods once reconnected to the hub.
  - **Mic Mute Grouping:** Slide the toggle to the right to enable or left to disable the mic mute grouping. If enabled, the **Mic Mute** function in the pod status table will sync across the paired pods. If disabled, the **Mic Mute** function in the pod status table will be accessed independently for the respective pods.
  - **System Mic Mute:** Slide the toggle to the right to enable or left to disable the system mic mute. If enabled, the **Mic Mute** function will sync across the entire system, including the paired pods, and the UC Engine or laptop. If disabled, the **Mic Mute** function will be accessed independently for the respective pods, the UC Engine or the laptop.
  - **Locate Audio Tone:** Slide the toggle to the right to enable the audio tone function for locating the paired pods. When **Locate All** is selected, the **Locate** tab in the pod status table is activated for the paired pods. The LED ring of the paired pods then starts blinking blue (rapidly and continuously) with an audio tone indicating the location of the respective pods.

- **Pod Status**

  The pod status table displays the following:

  - **Pod#:** Pod number
  - **Name:** An auto-generated pod name which can be renamed
  - **Status:** Displays if the pod is within the hub's range
  - **IPEI:** The pod unique identifier
  - **Trim:** The volume level for individual pod can be adjusted with **Trim**. Increase or decrease the volume level of the respective pod using the upper and lower arrows.
  - **Mic Mute:** The pod mic mute status. This functions in a group if the **Mic Mute Grouping** is enabled or functions independently for respective pods if **Mic Mute Grouping** is disabled.
  - **Audio Status:** Displays the active or inactive audio status of the pod speaker
  - **Signal Strength:** The pod DECT signal strength
  - **Firmware Version:** The pod firmware version
  - **Firmware Upgrade:** Pods are automatically upgraded when the paired hub's firmware is upgraded.
  - **Locate:** When **Locate All** is selected, the **Locate** tab in the pod status table is activated for the paired pods. The LED ring of the paired pods then starts blinking blue (rapidly and continuously) with an audio tone indicating the location of the respective pods.
  - **Unpair/Remove:** A pod can be unpaired or removed from the hub's connection by selecting the **Unpair/Remove** option.

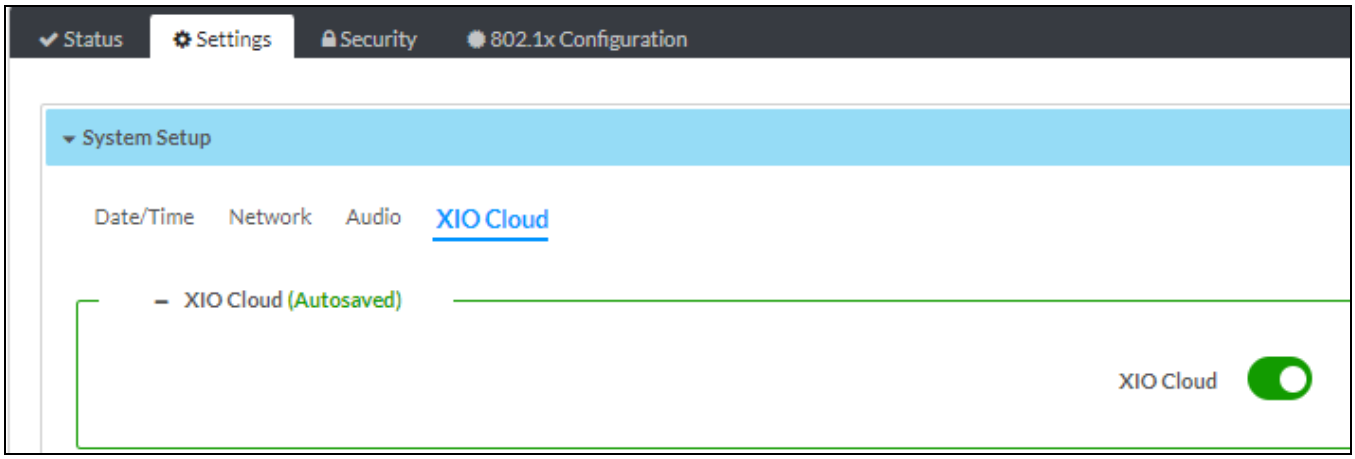
- **Upgrade All:** Pods are automatically upgraded when the paired hub's firmware is upgraded.
- **Locate All:** When **Locate All** is selected, the **Locate** tab in the pod status table is activated for the paired pods. The LED ring of the paired pods then starts blinking blue (rapidly and continuously) with an audio tone indicating the location of the respective pods.
- **Unpair All:** When **Unpair All** is selected, the **Unpair/Remove** tab in the pod status table is activated for the paired pods.

> **NOTE: Firmware Upgrade** and **Upgrade All** are not available with the initial launch of these products. These features will be available at a later date.

XiO Cloud

Select the + (plus) icon next to **XIO Cloud (Autosaved)** to display the following XiO Cloud settings.

Settings Tab - System Setup (XiO Cloud)



XiO Cloud settings is auto saved.

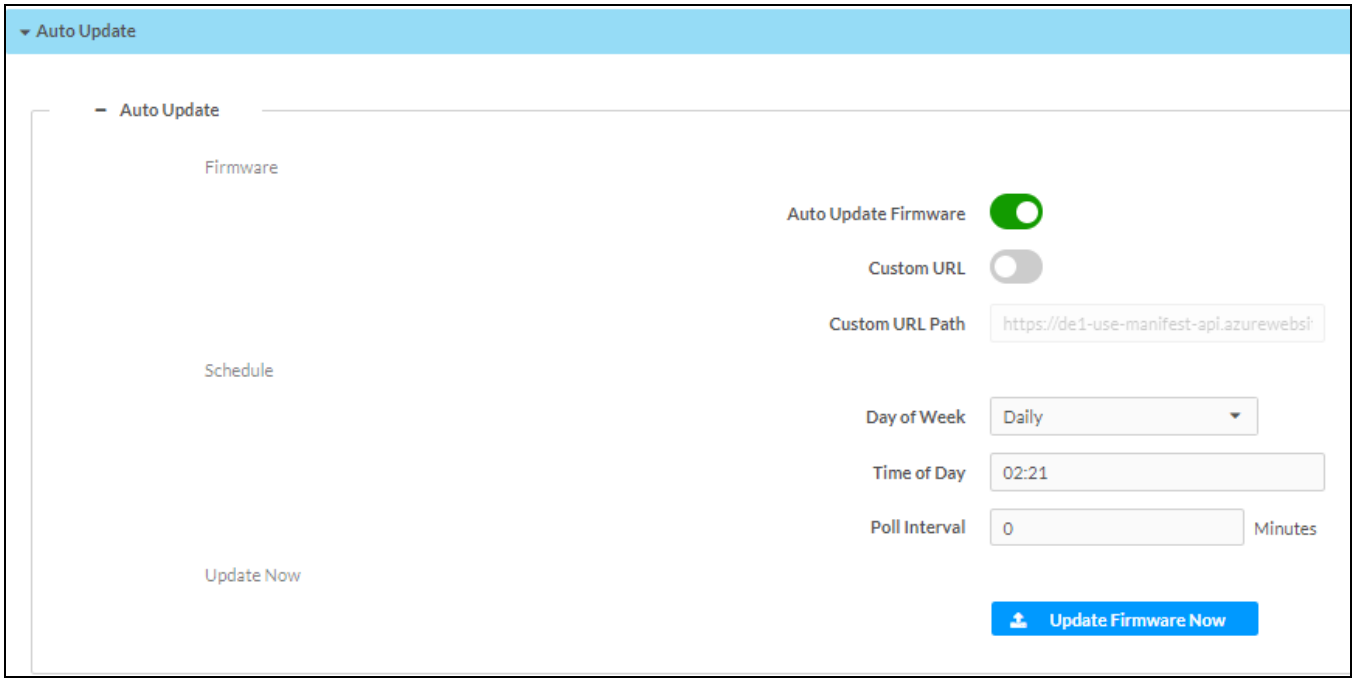
XIO Cloud: Slide the toggle to the right to enable or left to disable the XiO Cloud option

For more information on connecting to the XiO Cloud service, refer to XiO Cloud Service on page 61.

Auto Update

Select **Auto Update** to display the following auto update settings. The hub can be automatically updated with the latest firmware at scheduled intervals.

Settings Tab - Auto Update



Select the + (plus) icon next to **Auto Update** to display the following auto update settings.

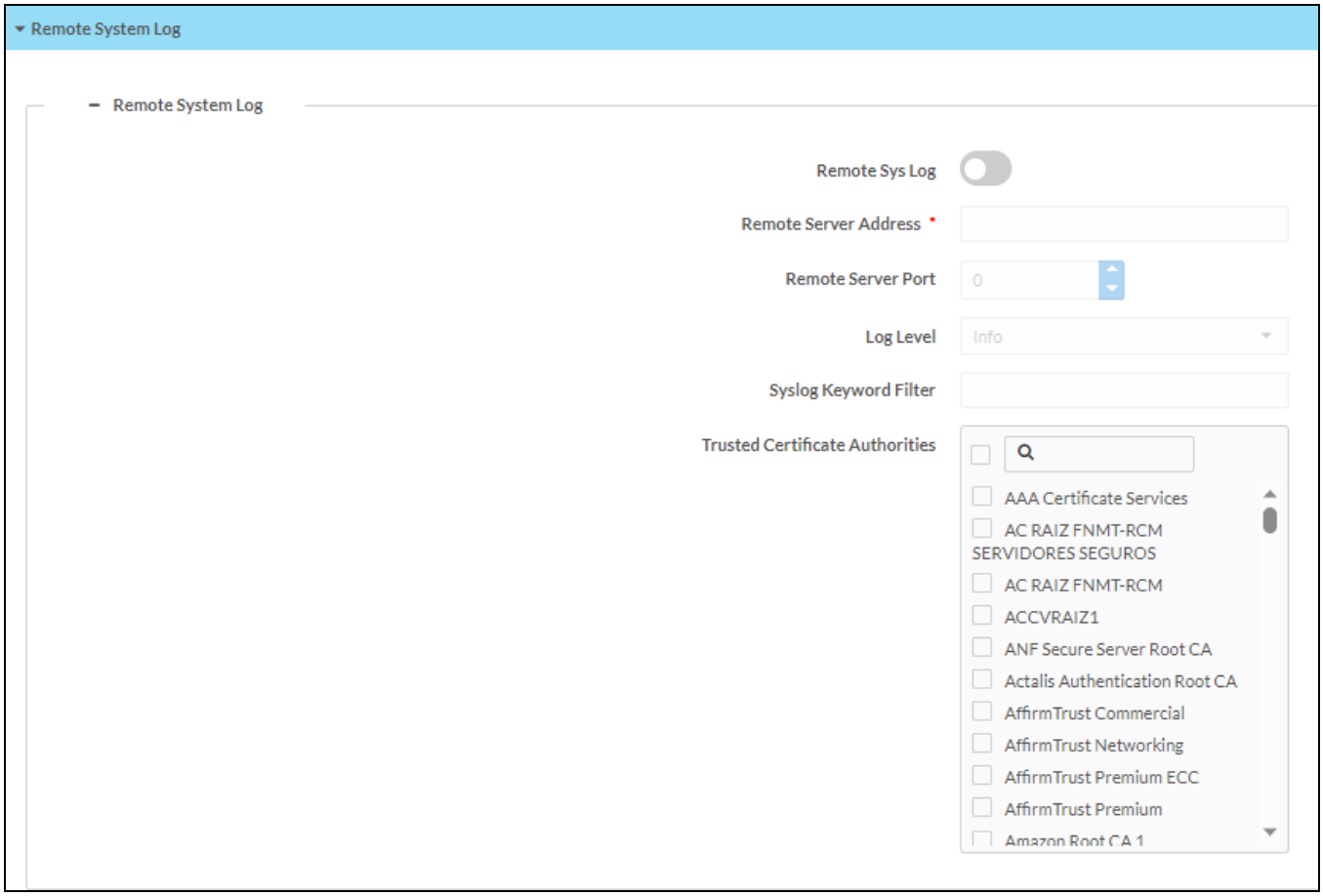
- **Firmware:** The hub firmware update
  - **Auto Update Firmware:** Slide the toggle to the right to enable auto update.
  - **Custom URL:** Slide the **Custom URL** toggle to the right (enable) or left (disable).
    - **Enabled:** If the Custom URL is enabled, enter the custom URL path for the updated server.
    - **Disabled:** If the Custom URL is enabled, use the default URL to download the updates from the Crestron server.
  - **Custom URL Path:** Enter the custom URL path into the text field.
- **Schedule:** Schedule auto update for the hub
  - **Day of Week:** Select the day of week using the drop-down arrow.
  - **Time of Day:** Enter the time of day in the 24-hour format.
  - **Poll Interval:** Enter the poll interval with a value from 60 to 65535 minutes. A value of 0 disables the Poll Interval.

  Select the **Save Changes** button displayed on the top right to save the auto update entries.
- **Update Firmware Now:** Selecting **Update Firmware Now** causes the firmware to be updated at the current time. However, the scheduled day of week, time of day and the poll interval remain in effect.

Remote System Log

Select **Remote System Log** to display the remote system log settings. Control system messages can be captured and stored on a remote server using the remote system logging function.

Settings Tab - Remote System Log



Select the **+** (plus) icon next to **Remote System Log** to display the following:

- **Remote System Log:** Slide the toggle to the right to enable the remote system log.
- **Remote Server Address:** Enter the IP address or Fully Qualified Domain Name (FQDN) in the Remote Server Address.
- **Remote Server Port:** Enter the port number in the Remote Server Port. The range is 0 to 65535.

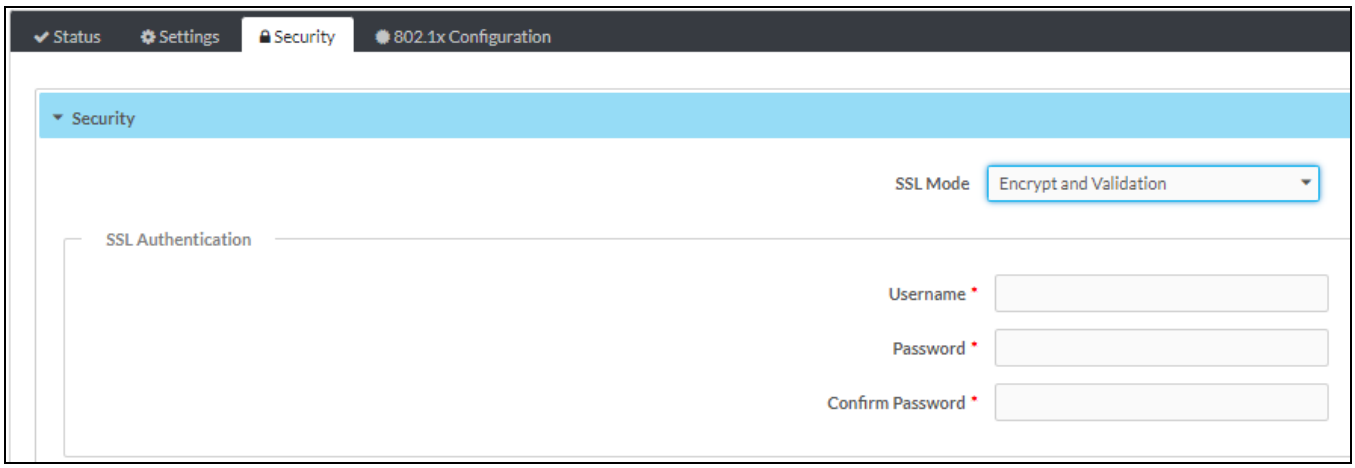
- **Log Level:** Select a log level for syslog. The default setting is **None**. There are four levels to select from the drop-down list, **DEBUG**, **INFO**, **WARNING**, and **ERROR**. Syslog messages are sent based on the following events:
    - Product model/version on boot up (INFO level)
    - NAT related info (INFO level)
    - Sent or received SIP message (DEBUG level)
    - SIP message summary (INFO level)
    - Inbound and outbound calls (INFO level)
    - Registration status change (INFO level)
    - Negotiated codec (INFO level)
    - Ethernet link up (INFO level)
    - SLIC chip exception (WARNING and ERROR levels)
    - Memory exception (ERROR level)
- **Syslog Keyword Filter:** Entering the Syslog Keyword Filter is optional. Syslog will be filtered based on the keywords provided. If multiple keywords are entered, it should be separated by a "comma." Please note that spaces are not allowed.
- **Trusted Certificate Authorities:** Select the trusted certificate authorities from the list.

Select the **Save Changes** button displayed on the top right to save the remote syslog entries.

Security

Select the **Security** tab on the top left of the interface to display security configuration selections for users and groups and to allow different levels of access to the hub functions.

Security Tab Selections



- **SSL Mode:** Select an SSL (Secure Sockets Layer) mode to use to establish a secure connection between the hub and the control system:
  - **Encrypt and Validation:** The hub will require a username and password to validate an encrypted SSL connection. Enter a username and password in the respective fields.
  - **Encrypt:** The hub will use an encrypted SSL connection.
  - **OFF:** The hub will not use an SSL connection.

User and group settings are also displayed under Security.

Current User

Select the **Current User tab** to view read-only information or to change the password for the current user.

Current User Tab



The following settings are displayed for the current user:

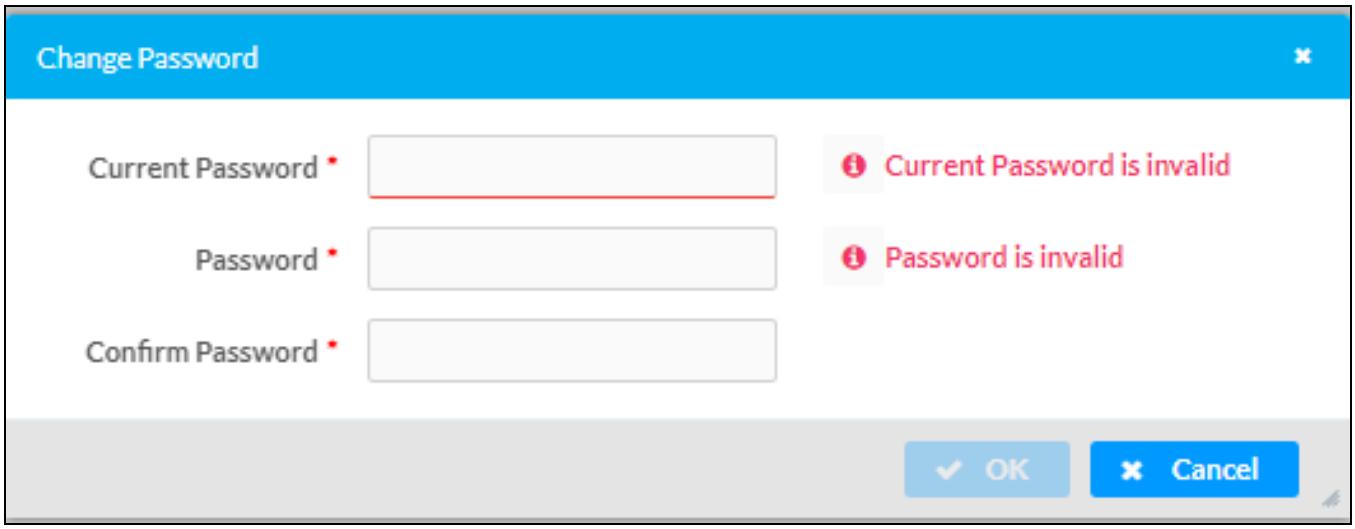
- **Name:** The chosen username
- **Access Level:** The access level granted to the user (Administrator, Programmer, Operator, User, or Connect)
- **Active Directory User:** Reports whether the current user is **(Yes)** or is not **(No)** authenticated through Active Directory® software

  > **NOTE:** A user must be added to an Active Directory group before the user is selected as an active directory user. For more information, refer to Groups on page 56.

- **Groups:** Any groups of which the current user is a member

Select **Change Current User Password** to change the password for the current user. The **Change Password** dialog box is displayed.

Change Password - Dialog Box

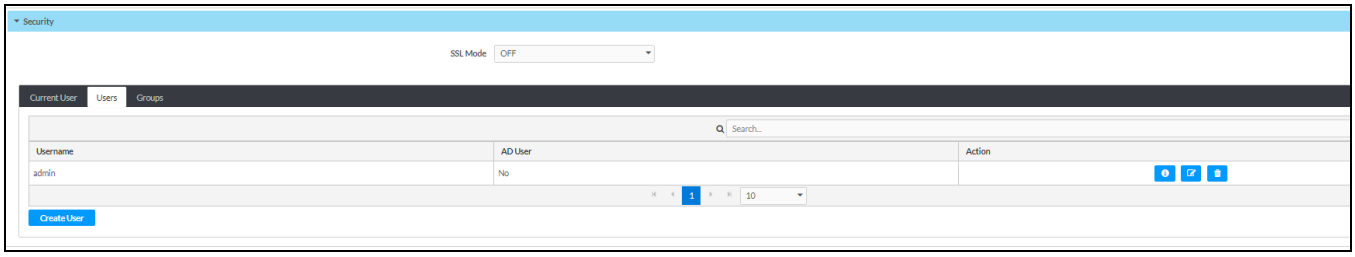


1. Enter the existing password in the **Current Password** field.
2. Enter a new password in the **Password** field, and re-enter the password in the **Confirm Password** field.
3. Select **OK** to save the new password, or select **Cancel** to cancel the change.

Users

Select the **Users** tab to view and edit information for the hub users.

Users Tab



Enter text into the **Search Users** field to find and display users that match the search term(s).

Hub users are listed in table format. The following information is displayed for each hub user:

- **Username:** The chosen username
- **AD User:** Reports whether the user is **(Yes)** or is not **(No)** authenticated through Active Directory

> **NOTE:** A user must be added to an Active Directory group before the user may be selected as an active directory user. For more information, refer to Groups on page 56.

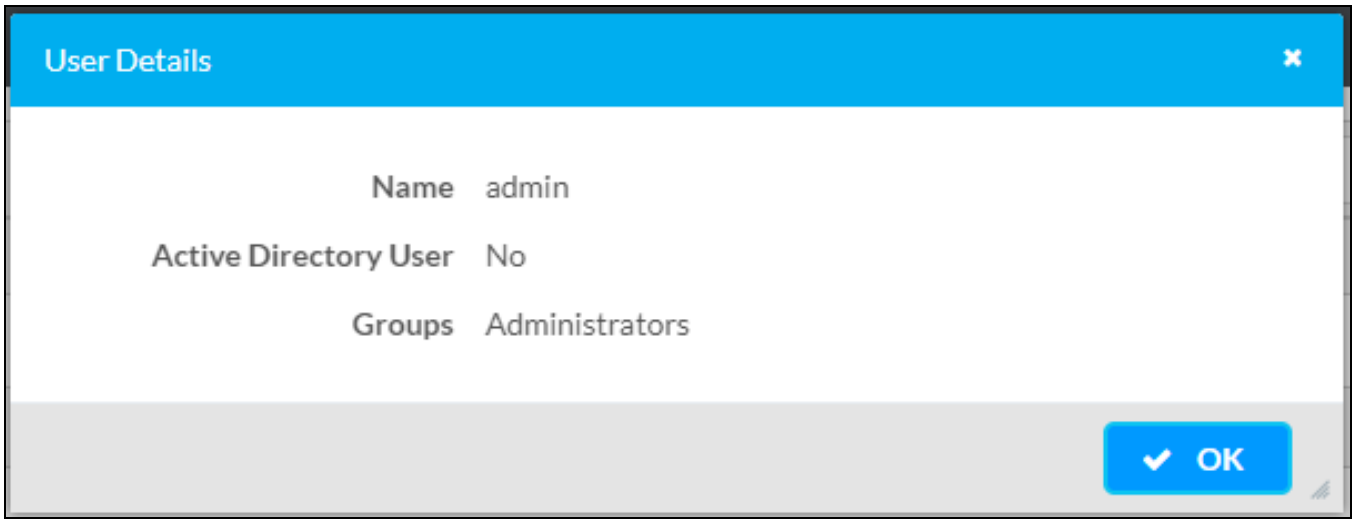
If the hub users span multiple pages, use the navigation arrows on the bottom of the page to move forward or backward through the pages, or select a page number to navigate to that page. Additionally, the number of users displayed on each page may be set to 5, 10, or 20 users.

An **Action** column is also provided for each user that allows various actions to be performed. The following selections may be selected from the Action column.

User Details

Select the information button in the **Actions** column to view information for the selected user. The **User Details** pop-up dialog box is displayed.

User Details Dialog Box



The following settings are displayed for the current user:

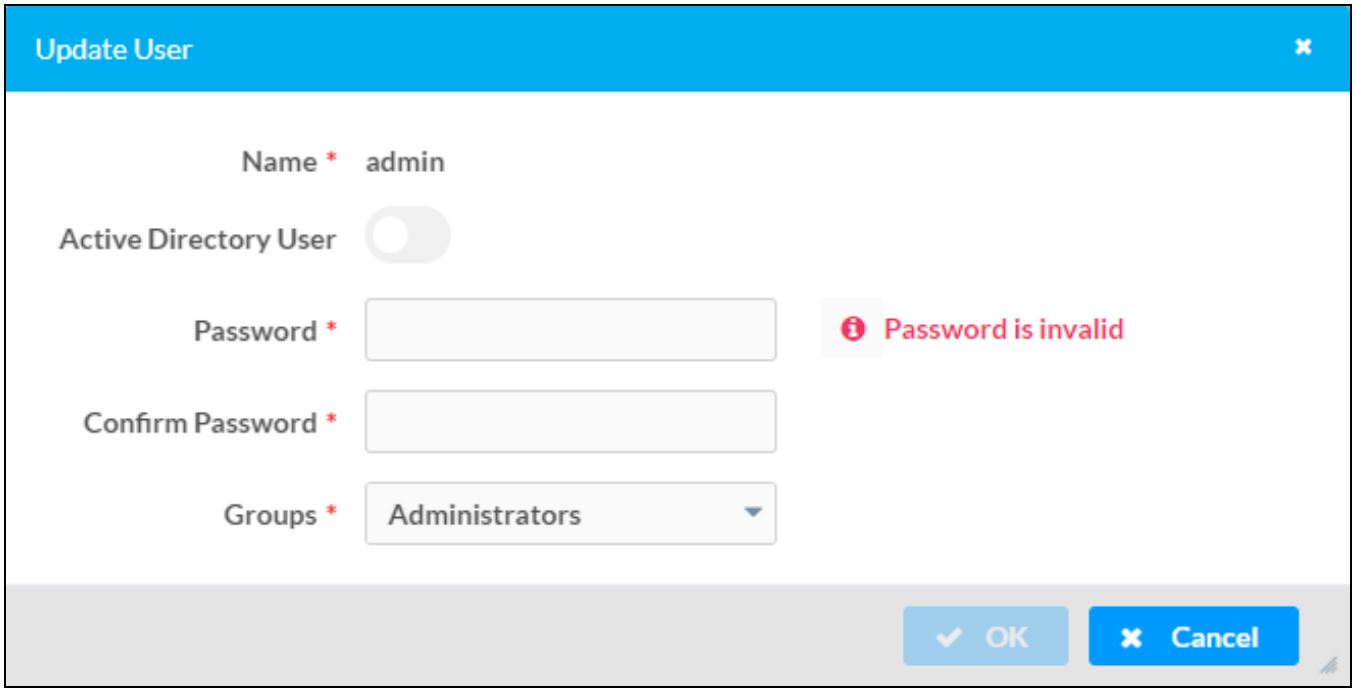
- **Name:** The chosen username
- **Active Directory User:** Reports whether the user is **(Yes)** or is not **(No)** authenticated through Active Directory
- **Groups:** Lists any groups that contain the user

Select **OK** to return to the **Users** page.

Update User

Select the editing button in the **Actions** column to edit settings for the selected user. The **Update User** dialog box is displayed.

Update User Dialog Box



The following **Update User** settings may be viewed or configured:

- **Name:** The chosen username
- **Active Directory User:** Slide the toggle to the right to use authentication via Active Directory for the selected user.
- **Password:** Enter a new password for the selected user.
- **Confirm Password:** Re-enter the password provided in the **Password** field.
- **Groups:** Add the user to one or more groups. For more information, refer to Groups on page 56.

> **NOTE:** A user must be added to an Active Directory group to be selected as an Active Directory user.

Select **OK** to save any changes and to return to the **Users** page. Select **Cancel** to cancel any changes.

Delete User

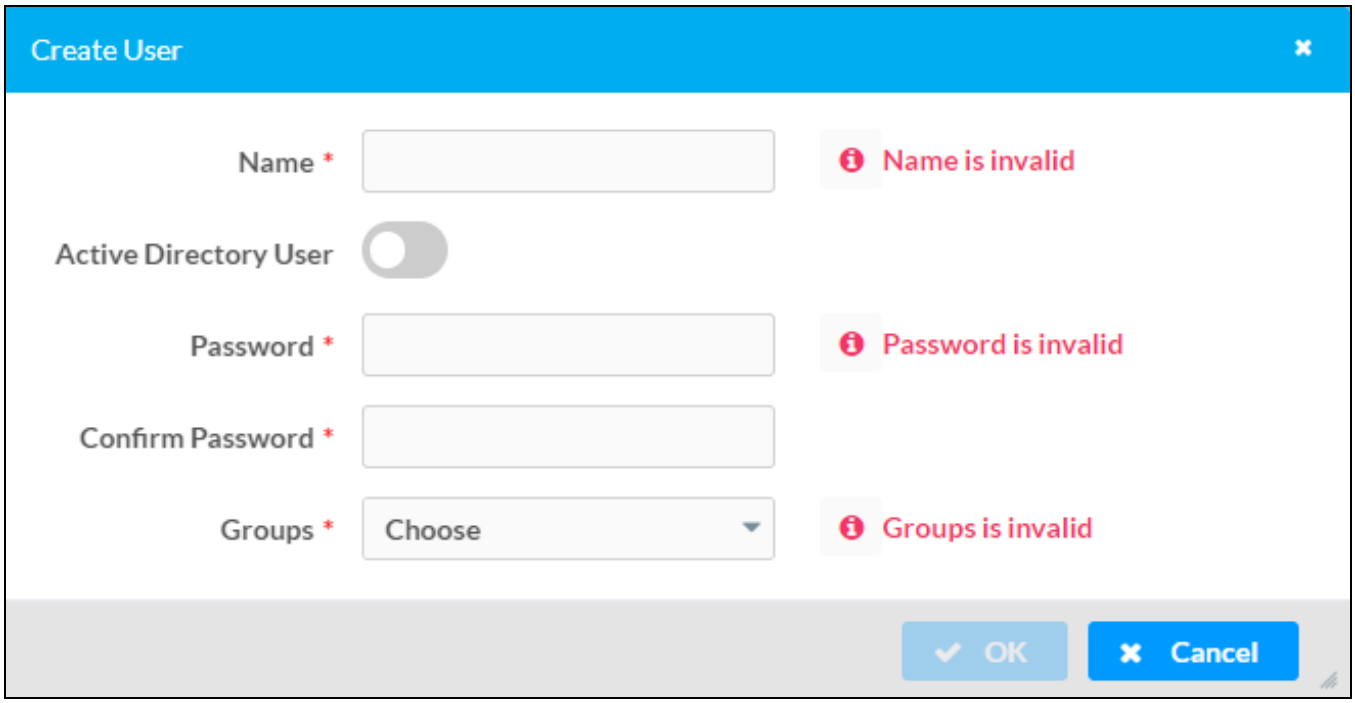
Select the trashcan icon in the **Action** column to delete the user.

A pop-up dialog box is displayed asking whether the user should be deleted. Select **Yes** to delete the user or **No** to cancel deleting the user.

Create User

Select **Create User** at the bottom of the page to create a new hub user. The **Create User** dialog box is displayed.

Create User Dialog Box



The following **Create User** settings are displayed:

- **Name:** Enter a username.
- **Active Directory User:** Slide the toggle to the right to use authentication via Active Directory for the user.
- **Password:** Enter a password for the user.
- **Confirm Password:** Re-enter the password provided in the **Password** field.
- **Groups:** Add the user to one or more groups. For more information, refer to Groups on page 56.

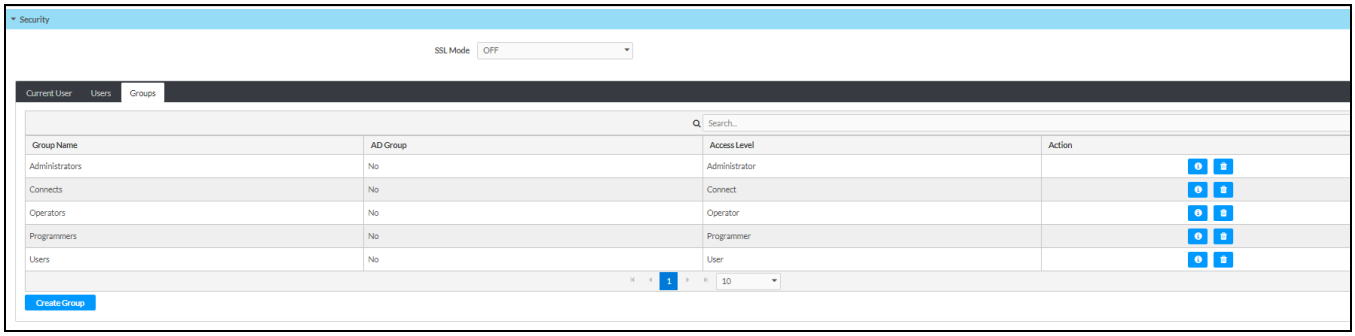
> **NOTE:** A user must be added to an Active Directory group to be selected as an Active Directory user.

Select **OK** to save any changes and to return to the **Users** page. Select **Cancel** to cancel creating a new user.

Groups

Select the **Groups** tab to view and edit settings for hub groups. Hub groups are used to group users by access level and Active Directory authentication settings.

Groups Tab



Enter text into the **Search Groups** field to find and display groups that match the search term(s).

Hub groups are listed in table format. The following information is displayed for each hub group:

- **Group Name:** The chosen group name
- **AD Group:** Reports whether the group is (**Yes**) or is not (**No**) authenticated through Active Directory

  > **NOTE:** Active Directory provides an additional layer of authentication for hub groups and users. Active directory group and usernames are stored in the hub console along with a unique SID (security identifier). When an Active Directory user attempts to authenticate against the console, the console first checks the user credentials. If the Active Directory authentication is successful, Active Directory queries the console for the user or group's SID. The user is granted access to the hub only if at least one SID match is found.

- **Access Level:** The access level for the selected group (**Administrator**, **Programmer**, **Operator**, **User**, or **Connect**)

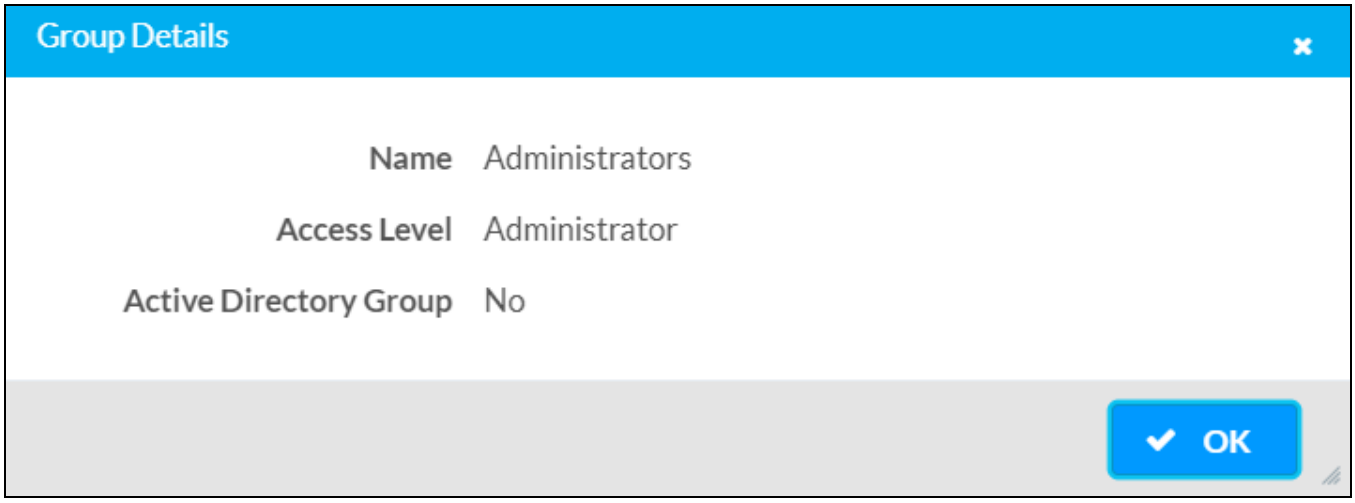
If the hub groups span multiple pages, use the navigation arrows on the bottom of the page to move forward or backward through the pages, or select a page number to navigate to that page. Additionally, the number of groups displayed on each page may be set to 5, 10, or 20 users.

An **Action** column is also provided for each group that allows various actions to be performed. The following selections may be selected from the **Action** column.

Group Details

Select the information button in the **Action** column to view information for the selected group. The **Group Details** dialog box is displayed.

Group Details Dialog Box



The following settings are displayed for the current group:

- **Name:** The chosen group name
- **Access Level:** The access level of the group and its users
- **Active Directory User:** Reports whether the group is (**Yes**) or is not (**No**) authenticated through Active Directory

Select **OK** to return to the **Groups** page.

Delete Group

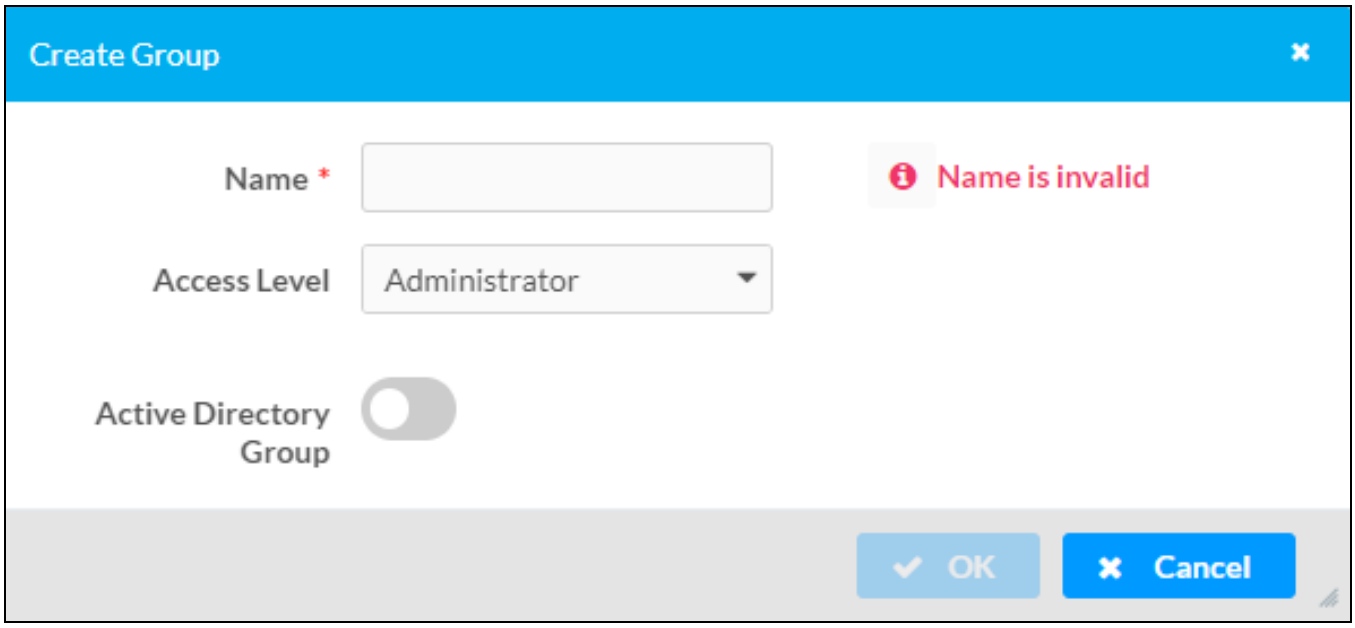
Select the trashcan icon in the **Actions** column to delete the group.

A pop-up dialog box is displayed asking whether the group should be deleted. Select **Yes** to delete the group or **No** to cancel deleting the group.

Create Group

Select **Create Group** at the bottom of the page to create a new hub group. The **Create Group** dialog box is displayed.

Create Group Dialog Box



Use the following settings to create a new group:

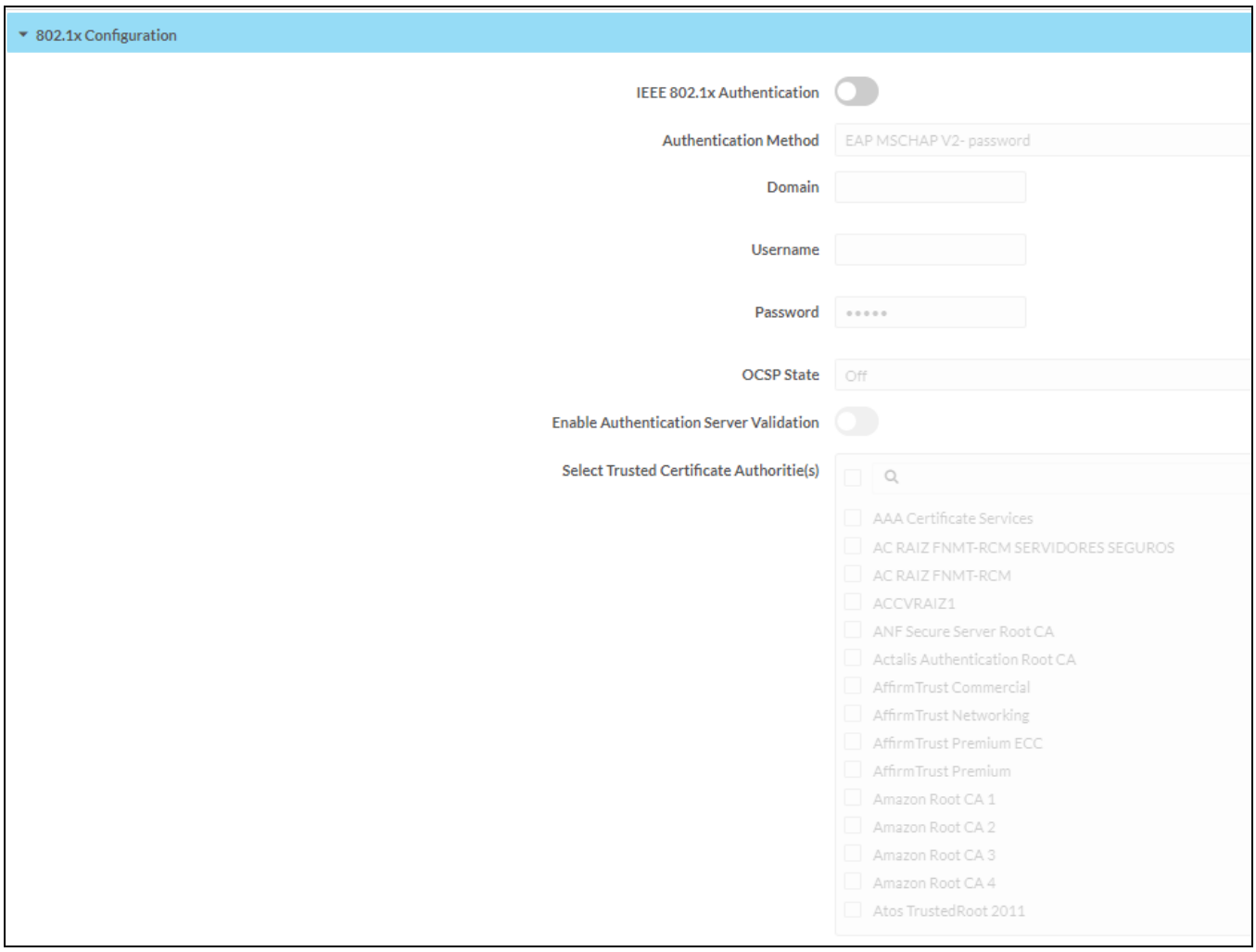
- **Name:** Enter a group name.
- **Access Level:** Select an access level for the group and its users from the drop-down menu.
- **Active Directory Group:** Slide the toggle to the right to use authentication via Active Directory for the group.

Select **OK** to save any changes and to return to the **Groups** page. Select **Cancel** to cancel creating a new group.

802.1x Configuration

Select the **802.1x Configuration** tab on the top left of the configuration interface to display selections for configuring IEEE 802.1X network authentication for hub security.

802.1x Configuration Tab Selections



Expand the **802.1x Configuration** accordion to configure the following settings:

- **IEEE 802.1x Authentication:** Slide the toggle to the right to use 802.1X authentication for the hub.
- **Authentication Method:** Select an 802.1X authentication method (**EAP-TLS Certificate** or **EAP MSCHAP V2- password**) from the drop-down menu.
- **Domain:** If **EAP MSCHAP V2- password** is selected for **Authentication Method**, enter a domain name that is required for authentication.
- **Username:** If **EAP MSCHAP V2- password** is selected for **Authentication Method**, enter a username that is required for authentication.
- **Password:** If **EAP MSCHAP V2- password** is selected for **Authentication Method**, enter a password that is required for authentication.

- **Enable Authentication Server Validation:** Turn on the toggle to use server validation for increased security.
- **Select Trusted Certificate Authorities:** Select trusted CAs (Certificate Authorities) from the provided CAs to be used for server validation:
    - Select the check box to the left of a CA to select it as a trusted CA.
    - Enter a search term into the text field at the top of the CA menu to search for and display CAs that match the search term.
    - Select the check box to the left of the search field at the top of the CA menu to select all CAs as trusted CAs.

Select **Manage Certificates** from the **Action** menu to add or remove CAs from the list. The **Manage Certificates** dialog box is displayed with the **Root** tab selected. For more information, refer to Manage Certificates on page 36.

XiO Cloud Service

The XiO Cloud® service allows supported devices across an enterprise to be managed and configured from one central and secure location in the cloud. Supported Crestron® devices are configured to connect to the service out of the box.

Use of the service requires a registered XiO Cloud account. To register for an XiO Cloud account, refer to https://www.crestron.com/Legal/XiO-Cloud-Monitoring-Services-TOU

NOTE: The device may be disconnected from the XiO Cloud service by navigating to the **Cloud Services** tab in Crestron Toolbox™ software (**Functions > Device Info > Cloud Services**). For details, refer to the Crestron Toolbox help file.

To connect the device to the XiO Cloud service:

1. Record the MAC address and serial number that are labeled on the shipping box or the device. The MAC address and serial number are required to add the device to the XiO Cloud service.

   NOTE: If the device has multiple MAC addresses, use the MAC address that is providing the primary connection back to the network. For most devices, the Ethernet MAC address should be used. However, if your device is connecting to the network over a different protocol (such as Wi-Fi® communications), use the MAC address for that protocol instead.

2. Log in to your XiO Cloud account at portal.crestron.io.
3. Claim the device to the XiO Cloud service as described in the XiO Cloud User Guide.

Select the device from the cloud interface to view its status and settings. The device may now also be managed and assigned to a group or room. For more information, refer to the XiO Cloud User Guide.

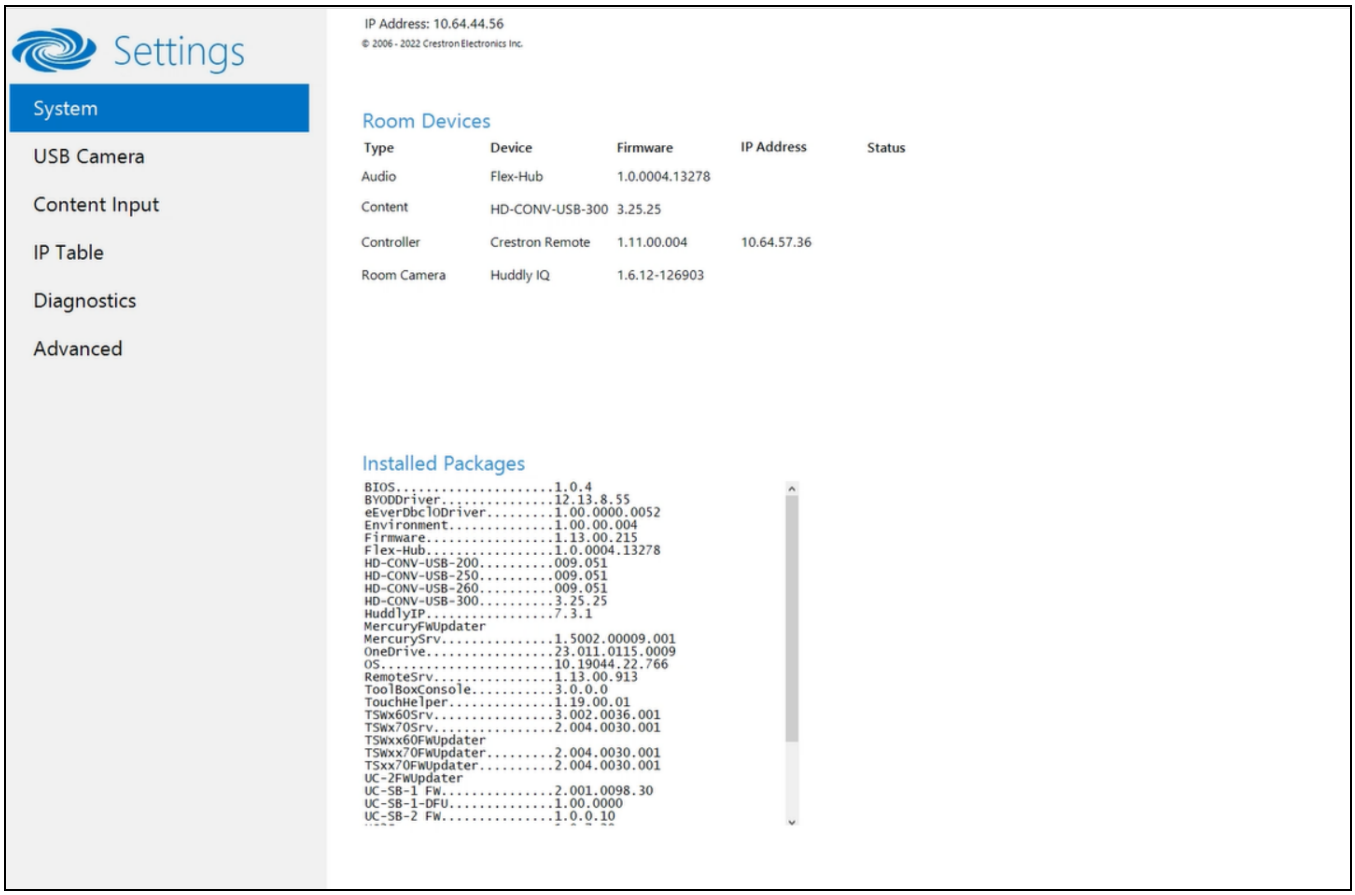
NOTE: For XiO Cloud accounts with room-based licenses, the device must be added to a licensed room before its status and settings can be viewed.

Crestron Settings App

The hub web user interface can be accessed through the Crestron Settings App if the hub is connected to a UC Engine. Crestron recommends using a keyboard and mouse connected to the UC Engine when using the Crestron Settings app.

To open the Crestron Settings App, click > **Crestron** folder > **Crestron Settings**. The Crestron Settings app opens.

NOTE: When opening the Crestron Settings app for the first time, you must agree to the CRESTRON UNIFIED COMMUNICATIONS SOFTWARE LICENSE AGREEMENT. Click **I Agree** to continue to the Crestron Settings app.



System

Use the **System** menu to view firmware versions of connected room devices and the firmware packages stored on the UC Engine.



Installed Packages

The hub firmware version is listed as **Flex-Hub** under installed packages.

- Click **Open Admin Page** to access the web UI.

  NOTES:

  - The Open Admin Page button and the IP address are not displayed if the hub is not connected to the network but shown on the list.
  - If the hub is connected to a UC Engine, auto-update is disabled even if it is connected to the network.

- Click **Done** to exit the Crestron Settings app.

Resources

The following resources are provided for the UC-AUDIO-POD and UC-AUDIO-HUB.

> **NOTE:** You may need to provide your Crestron.com web account credentials when prompted to access some of the following resources.

Crestron Support and Training

- Crestron True Blue Support
- Crestron Resource Library
- Crestron Online Help (OLH)
- Crestron Training Institute (CTI) Portal

Programmer and Developer Resources

- help.crestron.com: Provides help files for Crestron programming tools such as SIMPL, SIMPL#, and Crestron Toolbox™ software
- developer.crestron.com: Provides developer documentation for Crestron APIs, SDKs, and other development tools

Related Documentation

XiO Cloud User Guide

This page is intentionally left blank.

Crestron Electronics, Inc.
15 Volvo Drive, Rockleigh, NJ 07647
Tel: 888.CRESTRON
Fax: 201.767.7656
www.crestron.com

Product Manual — Doc. 9392B
11/27/23
Specifications subject to
change without notice.