



AirMedia® Series 3 Receivers

AM-3100-WF

AM-3100-WF-I

AM-3200

AM-3200-WF

AM-3200-WF-I

Product Manual

Crestron Electronics, Inc.

Original Instructions

The U.S. English version of this document is the original instructions.

All other languages are a translation of the original instructions.

Regulatory Models: M202018001, M202011001

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 at www.crestron.com/legal/patents.

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

Crestron, the Crestron logo, AirMedia, .AV Framework, Crestron Connected, Crestron Fusion, Crestron Studio, Crestron Toolbox, and XiO Cloud are either trademarks or registered trademarks of Crestron Electronics, Inc. in the United States and/or other countries. Apple, App Store, AirPlay, iPad, iPhone, Mac, macOS, and Safari are either trademarks or registered trademarks of Apple, Inc. in the United States and/or other countries. Appspace is either a trademark or a registered trademark of Appspace Inc. in the United States and/or other countries. Android, Chrome, Chrome OS, Google Calendar, Google Play, and YouTube are either trademarks or registered trademarks of Google, Inc. in the United States and/or other countries. iOS is either a trademark or registered trademark of Cisco Systems, Inc. in the United States and/or other countries. HDMI is either a trademark or registered trademark of HDMI Licensing LLC in the United States and/or other countries. Active Directory, Azure, Microsoft, Microsoft 365, Microsoft Edge, Microsoft Exchange Server, and Windows are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Firefox is either a trademark or registered trademark of the Mozilla Foundation in the United States and/or other countries. USB-C is either a trademark or registered trademark of USB Implementers. Miracast, Wi-Fi, and Wi-Fi Direct are either trademarks or registered trademarks 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.

©2022 Crestron Electronics, Inc.

Contents

Overview	1
Configuration	5
Web Configuration Interface	5
Connect to the Receiver	5
Action Menu	8
Status	15
Settings	24
Security	66
802.1x Configuration	72
Enterprise Deployment Options	75
XiO Cloud® Service	75
Crestron Deployment Tool for PowerShell® Software	76
Modern Authentication for EWS	76
Create the Application	77
Obtain Authentication IDs	80
Configure Additional Settings	80
Operation	87
Front of Room Experience	87
Welcome Screen	87
User Presentation	88
Present with AirMedia	89
Establish a Computer Connection	89
Share Content	91
Touch Screen Operation	104
Add a Touch Screen	104
Screen Controls	105
Room Scheduling	107
Present a Source	110
AirMedia Canvas	112

Overview

AirMedia® Series 3 receivers enable secure wireless collaboration in the modern digital workspace. Install the receivers in conference rooms, huddle rooms, lounges, lobbies, or almost any space to establish a productive meeting environment. This product manual discusses the requirements, configuration instructions, and operating instructions for AirMedia Series 3 receivers.

AirMedia Series 3 receivers are available in the following models:

- [AM-3100-WF](#): AirMedia Series 3 Receiver 100 with Wi-Fi® Network Connectivity
- [AM-3100-WF-I](#): AirMedia Series 3 Receiver 100 with Wi-Fi® Network Connectivity, International
- [AM-3200](#): AirMedia Series 3 Receiver 200
- [AM-3200-WF](#): AirMedia Series 3 Receiver 200 with Wi-Fi® Network Connectivity
- [AM-3200-WF-I](#): AirMedia Series 3 Receiver 200 with Wi-Fi® Network Connectivity, International

For more information on receiver features and capabilities, refer to [Feature Comparison \(on the facing page\)](#).

For installation information, refer to the following documents:

- [AM-3100-WF and AM-3100-WF-I Quick Start](#) (Doc. 8982A)
- [AM-3200, AM-3200-WF, and AM-3200-WF-I Quick Start](#) (Doc. 8986A)

For security and deployment information, refer to [AirMedia Presentation Gateway Security Reference Guide](#) (Doc 7693).

Feature Comparison

FEATURE	AM-3100-WF(-I)	AM-3200	AM-3200-WF(-I)
AirMedia Series 3 technology ¹	✓	✓	✓
AirMedia Output Resolution ²	1080p60	1080p60	1080p60
AirMedia Device Support			
Windows® OS (all versions)	✓	✓	✓
Mac® devices	✓	✓	✓
iPad® devices	✓	✓	✓
iPhone® devices	✓	✓	✓
iOS® devices	✓	✓	✓
Android™ devices	✓	✓	✓
AirMedia Screen Mirroring Support			
Windows® OS (all versions)	✓	✓	✓
Mac devices	✓	✓	✓
iPad devices	✓	✓	✓
iPhone devices	✓	✓	✓
iOS devices	✓	✓	✓
Android devices	✓	✓	✓
AirMedia Video + Audio Playback			
PC-Windows (all versions)	✓	✓	✓
Chrome OS™ operating system ³	✓	✓	✓
Mac devices	✓	✓	✓
iPad devices	✓	✓	✓
iPhone devices	✓	✓	✓
iOS devices	✓	✓	✓
Android devices	✗	✗	✗
AirMedia Playback Features			
DRM Content Support (Netflix, etc.)	✗	✗	✗
Device Internet Connection Required for AirPlay® Video Push	✓	✓	✓

FEATURE	AM-3100-WF(-I)	AM-3200	AM-3200-WF(-I)
Security			
AES-128/TLS security ⁴	✓	✓	✓
802.1X	✓	✓	✓
Active Directory® Authentication	✓	✓	✓
Crestron® Control			
.AV Framework™ Platform	✓	✓	✓
XiO Cloud® Service	✓	✓	✓
Crestron Studio® Software	N/A	N/A	N/A
SIMPL Windows	✓	✓	✓
SIMPL#	Future release	Future release	Future release
Virtual Control (VC-4)	✓	✓	✓
Video Inputs			
HDMI® Input	✗	1	1
HDMI Resolution	✗	1080p60	1080p60
HDMI HDCP	✗	HDCP 1.4	HDCP 1.4
Video Outputs			
HDMI Output	1	1	1
HDMI Resolution ⁵	4K60	4K60	4K60
HDMI HDCP	HDCP 2.2	HDCP 2.2	HDCP 2.2
Touch Screen Support	External	External	External
PoE Occupancy Sensor (CEN-ODT-C-POE)	✓	✓	✓
Other Interfaces			
COM/IR Support	✗	✓	✓
CEC	✓	✓	✓
Power Over Ethernet	✓	✓	✓
Direct Connect Scheduling Integration ⁶			
Microsoft Exchange Server® or Microsoft 365® Software	✓	✓	✓
Google Calendar™ Service	✓	✓	✓
General Features			
AirMedia Canvas	✓	✓	✓

FEATURE	AM-3100-WF(-I)	AM-3200	AM-3200-WF(-I)
Airmedia Canvas Control	✓	✓	✓
Control System Interface	✓	✓	✓
Wireless Conferencing	✓	✓	✓
Appspace® Application	✓	✓	✓
Wireless Access Point Mode	✓	✗	✓
Moderator Mode	Future release	Future release	Future release
AirMedia Connect Adapter	Future release	✗	Future release
YouTube® software Pushmode Support	✓	✓	✓
Mounting	Freestanding Surface	Freestanding Surface Rack	Freestanding Surface Rack
Dimensions	Height: 1.21 in. (31 mm) Width: 5 in. (127 mm) Depth: 5 in. (127 mm)	Height: 1.26 in. (33 mm) Width: 7.40 in. (188 mm) Depth: 6.93 in. (177 mm)	Height: 1.26 in. (33 mm) Width: 7.40 in. (188 mm) Depth: 6.93 in. (177 mm)

Notes:

1. To compare iterations of AirMedia technology, refer to the [AirMedia Presentation Gateway Security Reference Guide](#) (Doc 7693).
2. All video inputs are scaled to the HDMI output resolution.
3. The AirMedia Extension for Google Chrome OS relies on web technologies for screen sharing that are built into the web browser. Performance variations with motion video (quality and frame rate) will be observed based upon the encoding capabilities of the Chrome OS device and the nature of the content being displayed (ex. High motion video).
4. TLS 1.3 is not currently supported.
5. All video inputs are scaled to the HDMI output resolution.
6. Connection via Crestron Fusion® software may allow additional providers.

Configuration

To configure receiver settings using the web configuration interface, deploy multiple receivers across an enterprise, or enable Modern Authentication for EWS, refer to the following sections:

- [Web Configuration Interface \(below\)](#)
- [Enterprise Deployment Options \(on page 75\)](#)
- [Modern Authentication for EWS \(on page 76\)](#)

Web Configuration Interface

Configure the AirMedia receiver using the included web configuration interface.

To connect to the receiver and configure its settings, refer to the following sections:

- [Connect to the Receiver \(below\)](#)
- [Action Menu \(on page 8\)](#)
- [Status \(on page 15\)](#)
- [Settings \(on page 24\)](#)
- [Security \(on page 66\)](#)
- [802.1x Configuration \(on page 72\)](#)

Connect to the Receiver

To connect to the receiver's web configuration interface, a computer must be connected to the same network as the AirMedia receiver. The web configuration interface is accessible from a web browser. This interface is also accessible using the XiO Cloud® service.

Supported Web Browsers

When connecting to the receiver's web configuration interface, use one of the supported web browsers listed below.

Web Configuration Interface Supported Web Browsers

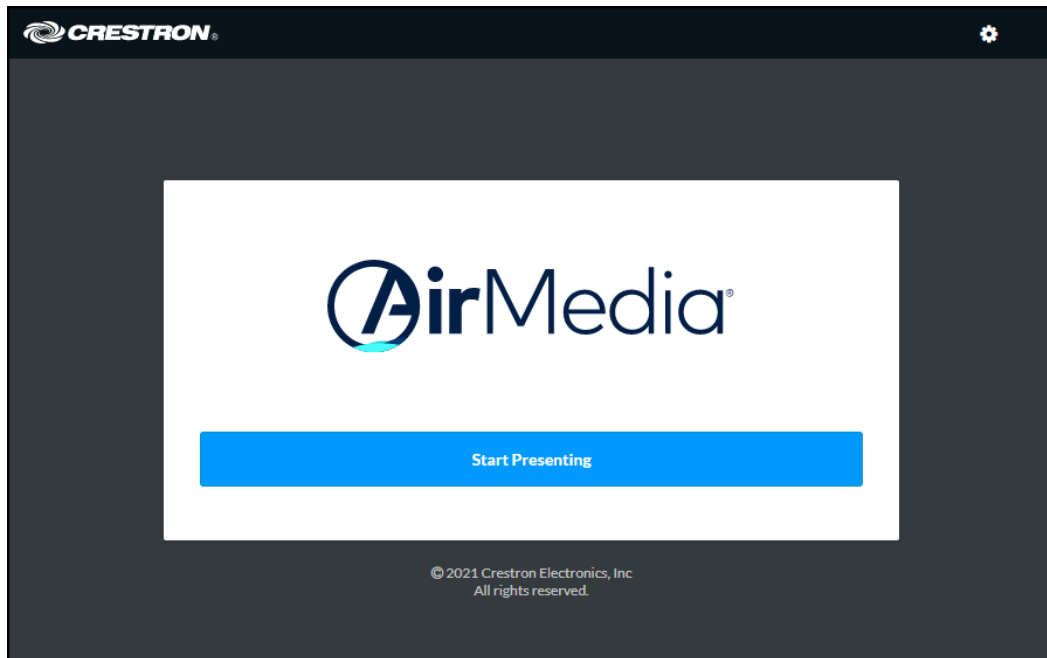
OPERATING SYSTEM	SUPPORTED WEB BROWSERS
Windows® operating system	Chrome™ web browser, version 31 and later
	Firefox® web browser, version 31 and later
	Microsoft Edge® web browser, version 86 and later
macOS® operating system	Chrome web browser, version 31 and later
	Firefox web browser, version 31 and later
	Safari® web browser, version 6 and later

Sign in to the Receiver

To connect to the receiver using the web configuration interface:

1. On a computer, open a web browser and navigate to the IP address or host name that is shown on the display device. The welcome screen is displayed.

Welcome Screen

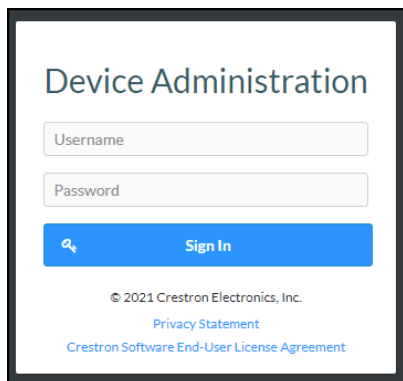


2. Select the settings button  in the title bar to log in.

NOTE: Prior to displaying the prompt for login credentials, the web browser may display a security warning message about the security certificate. It is safe to ignore this warning as long as the user verifies that the browser's address bar indicates the receiver IP address or host name as shown on the display device.

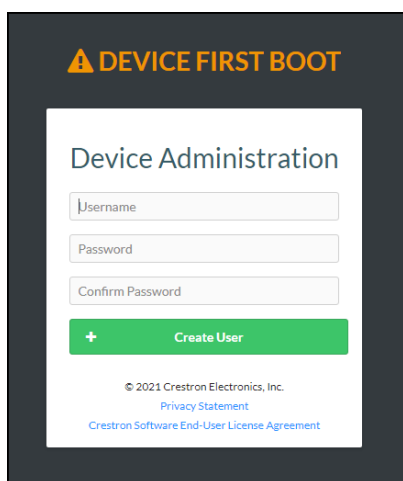
3. If this is a new sign-on, enter the new username and password in their respective fields and select **Create User** to continue. Otherwise, enter the username and password that were previously configured, and select **Sign In** to continue. The receiver's web configuration interface is displayed.

Login Screen



The image shows a web interface titled "Device Administration". It features two input fields: "Username" and "Password". Below these fields is a blue button with a magnifying glass icon and the text "Sign In". At the bottom, there is copyright information: "© 2021 Crestron Electronics, Inc.", followed by links for "Privacy Statement" and "Crestron Software End-User License Agreement".

Enter New User Name and Password



The image shows a web interface titled "Device Administration" with a dark background and a white central box. At the top of the box, there is an orange warning icon and the text "DEVICE FIRST BOOT". Inside the box, there are three input fields: "Username", "Password", and "Confirm Password". Below these fields is a green button with a plus icon and the text "Create User". At the bottom, there is copyright information: "© 2021 Crestron Electronics, Inc.", followed by links for "Privacy Statement" and "Crestron Software End-User License Agreement".

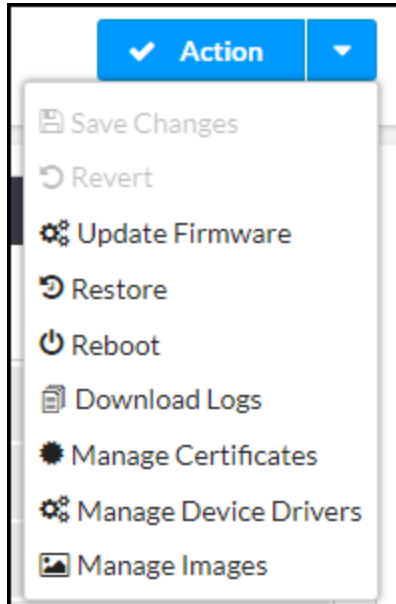
Log Out from the Receiver

Select **Sign Out** to log out of the receiver's web configuration interface and return to the welcome screen. If **Sign Out** is not selected, the user will be logged out automatically after 20 minutes of inactivity.

Action Menu

The web configuration interface provides an **Action** drop-down menu. The **Action** menu may be accessed at any time.

Action Menu



The **Action** menu provides the following selections.

Save Changes

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

If a reboot is required after changes have been saved, select **Yes** to reboot the device or **No** to cancel the reboot.

Revert

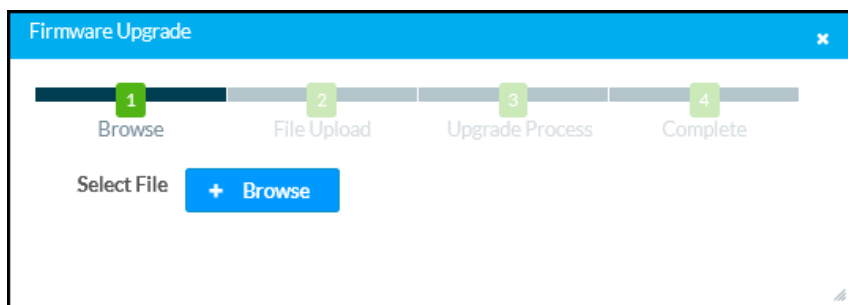
Select **Revert** to revert the receiver to the last saved configuration settings.

Update Firmware

To upgrade the device firmware manually with a downloaded PUF (package update file), select **Update Firmware**. The **Firmware Upgrade** dialog box opens.

NOTE: Visit crestron.com/firmware to download the latest firmware PUF.

Firmware Upgrade Dialog Box



To upload a firmware PUF through the web configuration interface:

1. Select **Browse**, and then navigate to the firmware PUF on the host computer.
2. Select the firmware PUF, and then select **Open**.
3. Select **Load** to load the PUF to the receiver. The upload progress is shown in the dialog box.
4. Once the device has completed the firmware upgrade, select **OK**.

Select the **x** button to close the **Firmware Upgrade** dialog box. Selecting the **x** button before the PUF is uploaded to the device cancels the upgrade. Once the PUF upload process begins, the dialog box cannot be closed, and the upload process cannot be canceled.

Restore

Select **Restore** to restore the device configuration settings to their default values. Select **Yes** to restore the settings or **No** to cancel the restore.

NOTE: If the device is restored to factory settings, the default user name and password used to configure the device will be restored as well. Any custom user names or passwords will no longer function.

Reboot

Select **Reboot** to reboot the device. Select **Yes** to reboot the device or **No** to cancel the reboot.

Download Logs

Select **Download Logs** to download the device 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.

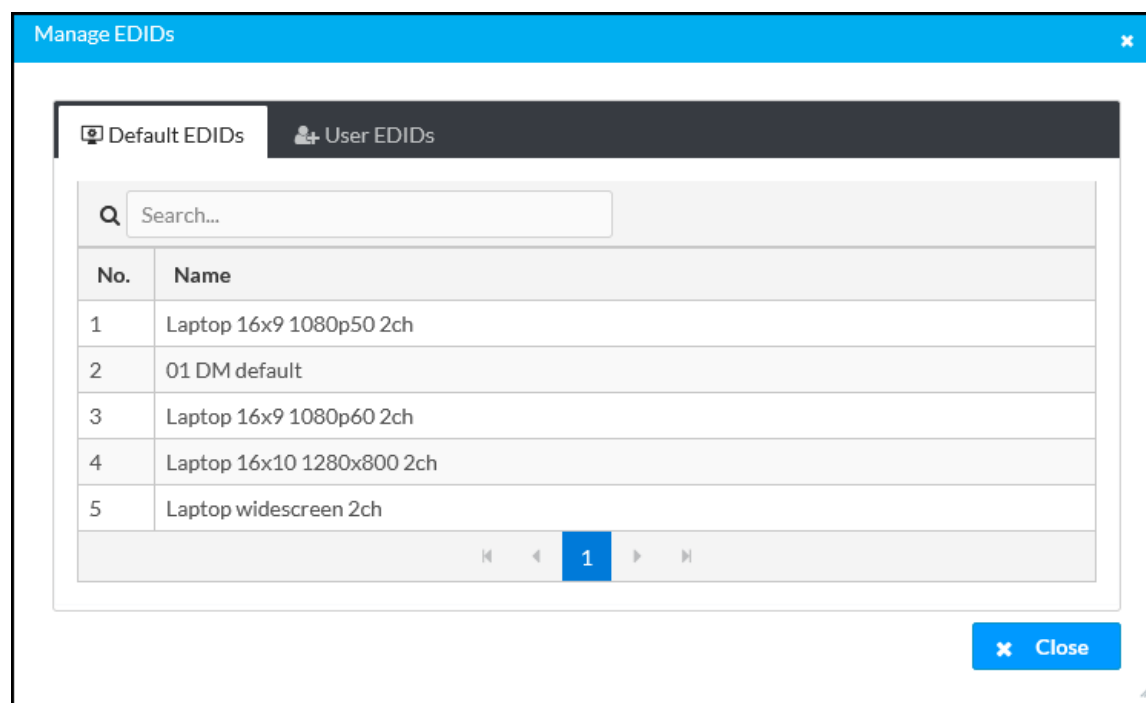
Manage EDIDs (AM-3200(-WF)(-I) Models Only)

Select **Manage EDIDs** to manage Extended Display Identification Data (EDID) profiles that are installed on the receiver. The **Manage EDIDs** window opens.

Default EDIDs

Select **Default EDIDs** to view EDIDs preinstalled on the receiver.

Manage EDIDs - Default EDIDs Tab



Enter text in the **Search...** field to find and display EDIDs that match the search term(s).

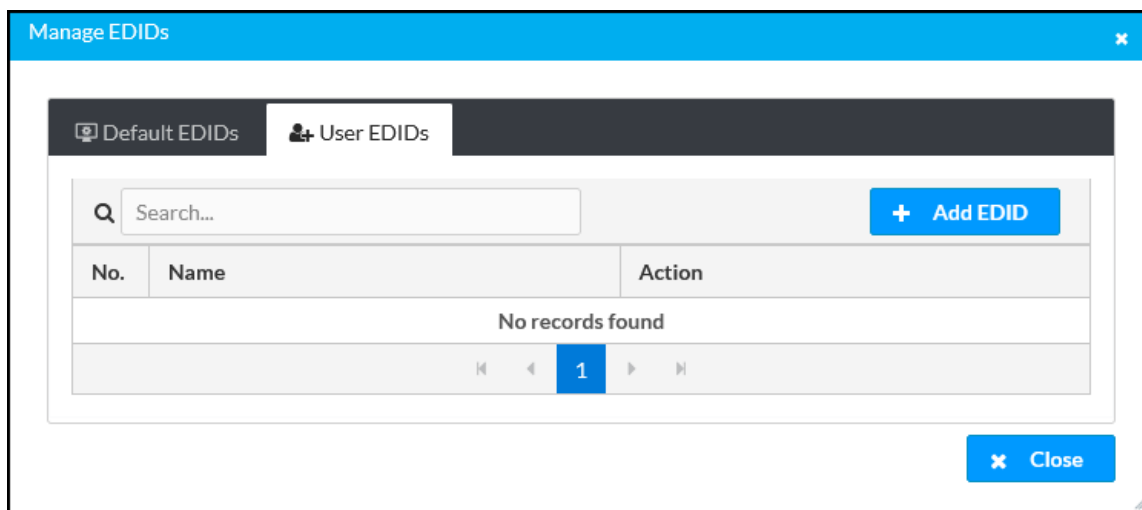
EDIDs are listed in table format. If the EDIDs span multiple pages, use the navigation arrows on the bottom of the page to move forward or backward through the pages, or select a page number to navigate to that page.

Select **Close** to close the **Manage EDIDs** window.

User EDIDs

Select **User EDIDs** to manage EDIDs installed by users.

Manage EDIDs - User EDIDs Tab



Enter text in the **Search...** field to find and display EDIDs that match the search term(s).

EDIDs are listed in table format. If the EDIDs 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.

To upload an EDID file:

1. Select **Add EDID**.
2. Select **Browse**.
3. Navigate to the EDID file on the host computer.
4. Select the EDID file, and then select **Open**.
5. Select **Load** to load the EDID file to the receiver. The upload progress is shown in the dialog box.
6. Once the receiver has completed the upload, select **OK**.

Select the trashcan button  in the **Action** column to delete the EDID. Select **Yes** to delete the EDID or **No** to cancel.

Select **Close** to close the **Manage EDIDs** window.

Manage Certificates

Select **Manage Certificates** to manage any certificates that are installed on the receiver. For more information on certificate management, refer to [802.1x Configuration \(on page 72\)](#).

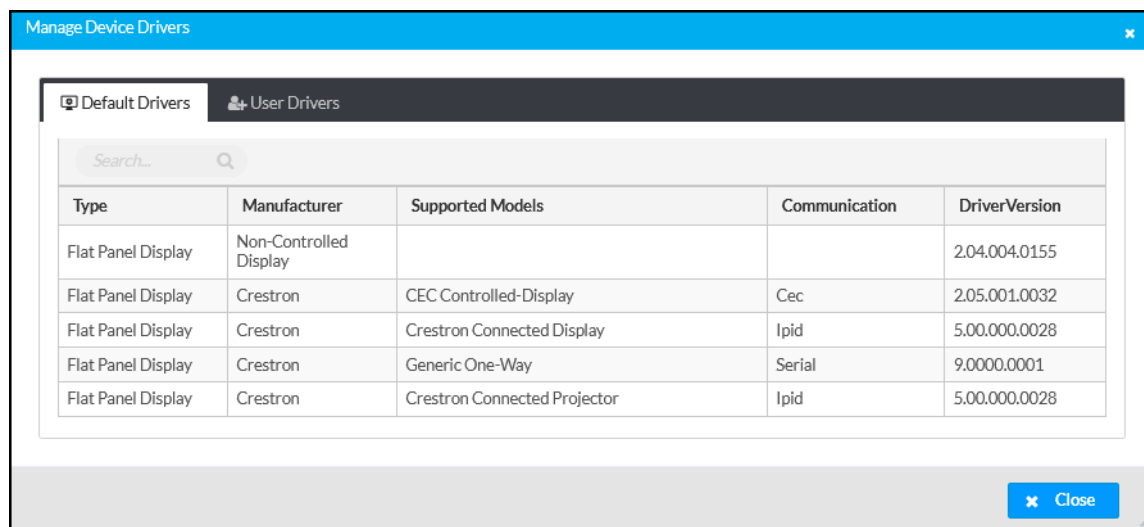
Manage Device Drivers

Select **Manage Device Drivers** to manage any drivers that are installed on the receiver. The **Manage Device Drivers** window appears. Support for CEC, Crestron Connected® control, IP, serial, and infrared profiles are built-in.

Default Drivers

Select **Default Drivers** to view information for the drivers preinstalled on the receiver.

Manage Device Drivers - Default Drivers Tab



Type	Manufacturer	Supported Models	Communication	DriverVersion
Flat Panel Display	Non-Controlled Display			2.04.004.0155
Flat Panel Display	Crestron	CEC Controlled-Display	Cec	2.05.001.0032
Flat Panel Display	Crestron	Crestron Connected Display	Ipid	5.00.000.0028
Flat Panel Display	Crestron	Generic One-Way	Serial	9.0000.0001
Flat Panel Display	Crestron	Crestron Connected Projector	Ipid	5.00.000.0028

Enter text in the **Search...** field to find and display drivers that match the search term(s).

Drivers are listed in table format. The following information is displayed for each driver:

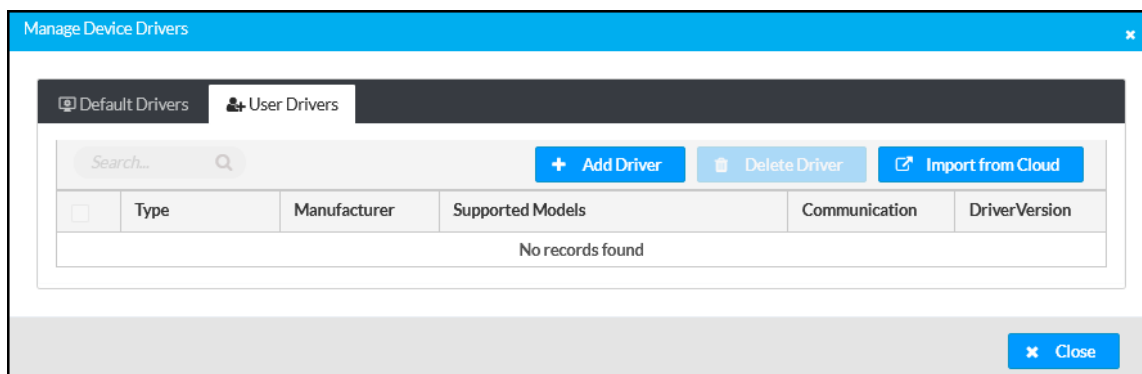
- **Type:** The supported display type (flat panel display, projector, etc.)
- **Manufacturer:** The driver manufacturer
- **Supported Models:** The display model name
- **Communication:** The driver communication type (Serial/RS-232, IR, IP, CEC)
- **DriverVersion:** The version of the installed driver

Select **Close** to close the **Manage Device Drivers** window.

User Drivers

Select **User Drivers** to manage drivers installed by users.

Manage Device Drivers - User Drivers Tab



Drivers are listed in table format. The following information is displayed for each driver:

- **Type:** The supported display type (flat panel display, projector, etc.)
- **Manufacturer:** The driver manufacturer
- **Supported Models:** The display model name
- **Communication:** The driver communication type (Serial/RS-232, IR, IP, CEC)
- **DriverVersion:** The version of the installed driver

Select **Close** to close the **Manage Device Drivers** window.

Add Driver

To upload a driver:

1. Select **Add Driver**.
2. Select **Browse**.
3. Navigate to the driver file on the host computer.
4. Select the driver file, and then select **Open**.
5. Select **Load** to load the driver file to the receiver. The upload progress is shown in the dialog box.
6. Once the receiver has completed the upload, select **OK**.

Delete Driver

To delete a driver from the receiver:

1. Locate the driver that you wish to delete in the driver table, and then select the corresponding checkbox.
2. Select **Delete Driver**.
3. Select **Yes** to delete the driver.

Import from Cloud

Crestron maintains a cloud-based driver database. To load drivers to the receiver from the cloud:

1. Select **Import from Cloud**.
2. Enter text in the **Search...** field to find and display drivers that match the search term(s).

3. Locate the driver that you wish to upload to the receiver, and then select the corresponding radio button .
4. Select **Add** to add the driver to the receiver.

Manage Images

Select **Manage Images** to add or remove images used as custom logo graphics or custom backgrounds.

NOTE: For more details on using custom logo graphics and custom backgrounds, refer to [Connected Devices \(on page 47\)](#).

Manage Images

Manage Images

Images Loaded 0 of 20

Storage Capacity 0 of 100 MB

+ Add

✕ Remove

☐	Index	File Name	Status	Preview
	1	<Empty>		
	2	<Empty>		
	3	<Empty>		
	4	<Empty>		
	5	<Empty>		

✕ Close

To add an image to the receiver:

NOTES:

- Up to 20 images can be loaded. The receiver's storage capacity is 100 MB.
- Custom background images should be jpg files with resolutions no higher than 4096 x 2304 pixels. Images with resolutions higher than 4096 x 2304 pixels may exceed the receiver's storage limit when rendered and will inhibit performance.

1. Select **Add**.
2. Select **Browse**, and then navigate to the image file on the host computer.
3. Select the image file, and then select **Open**.
4. Select **Load** to load the image to the receiver.
5. Once the receiver has completed the image upload, select **OK**.

Select the **x** button to close the **File Upload** dialog box at any time during the upgrade process. Selecting the **x** button before the image file is uploaded to the receiver cancels the upload.

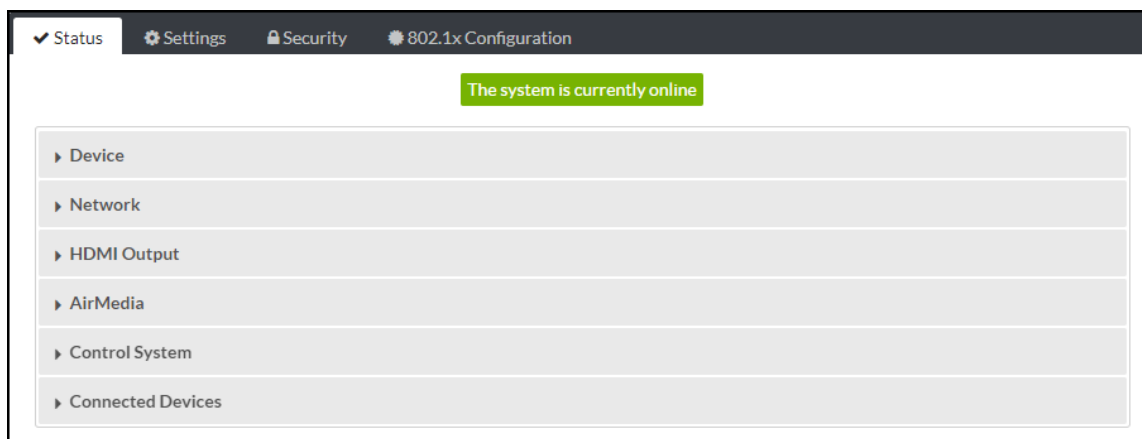
Once the image file is uploaded, the file's name, status, and preview will appear in the **Manage Images** table.

To remove an image from the receiver, select the checkbox in the corresponding table row, and then select **Remove**.

Status

Select **Status** to display selections for viewing the status of receiver, network, and control system settings. Select a section name to expand the menu. If the menu is expanded, select the section name again to collapse the section.

Status Screen



Device

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

Status – Device

▼ Device	
Model	AM-3100-WF
Serial Number	2104GSP00007
Firmware Version	2.0100.0015
Power Status	PoE
+ More Details	

The following **Device** information is displayed:

- **Model:** The receiver model name.
- **Serial Number:** The receiver serial number.
- **Firmware Version:** The firmware version loaded onto the receiver.
- **Power Status:** Displays how the device is currently being powered (DC, PoE, or PoE+).

Select **+ More Details** at the bottom of the tab to display an expanded section that shows additional information. Select **- More Details** to collapse the section.

Network

Select **Network** to view the status of the network settings for the receiver.

Status – Network

▼ Network

Hostname

AM-3200-WF-000000000000

Domain

hsd1.nj.comcast.net

DNS Servers

75.75.75.75(DHCP),75.75.76.76(DHCP)

– Adapter 1

DHCP

Yes

IP Address

10.0.0.238

Subnet Mask

255.255.255.0

Default Gateway

10.0.0.1

Link Active

True

MAC Address

00:10:7f:ed:7a:6c

+ Adapter 2

– Wireless Access Point

DHCP Enabled

Yes

SSID

IP Address

0.0.0.0

Subnet Mask

0.0.0.0

Default Gateway

0.0.0.0

Link Active

False

MAC Address

00:10:7f:ed:7a:6e

The following **Network** information is displayed:

- **Host Name:** The receiver hostname
- **Domain:** The receiver domain name
- **DNS Servers:** The DNS (domain name server) addresses used to resolve the receiver domain to an IP address

Select the + (plus) icon next to **Adapter 1** and/or **Adapter 2** to view the following DHCP server settings:

- **DHCP:** Reports whether the IP address is dynamic (Yes) or static (No)
- **IP Address:** The receiver IP address
- **Subnet Mask:** The receiver subnet mask
- **Default Gateway:** The gateway router address
- **Link Active:** Reports the status of the Ethernet connection. A true message indicates that the Ethernet connection is active, while a false message indicates that the Ethernet connection is inactive.
- **MAC Address:** The unique device MAC (media access control) address

Select the + (plus) icon next to **Wireless Access Point** to view the following wireless access point settings:

NOTE: Values are shown for the following settings only if a wireless access point is used.

- **DHCP Enabled:** Reports whether the IP address is dynamic (Yes) or static (No)
- **SSID:** The wireless access point network name
- **IP Address:** The wireless access point IP address
- **Subnet Mask:** The wireless access point subnet mask
- **Default Gateway:** The gateway router address
- **Link Active:** Reports the status of the Ethernet connection. A true message indicates that the Ethernet connection is active, while a false message indicates that the Ethernet connection is inactive.

HDMI Input (Receiver 200 Models Only)

Select **HDMI Input** to view the status of a device connected to the HDMI input.

Status – HDMI Input

▼ HDMI Input	
Sync Detected	No
Resolution	0x0@0
Source HDCP	Inactive
- More Details	
HDCP State	NonHdcpSource
Interlaced	No
Horizontal Resolution	0
Vertical Resolution	0
Frames Per Second	0
Aspect Ratio	No signal
Audio Format	No Audio
Audio Channels	0

The following HDMI Input information is displayed:

- **Sync Detected:** Indicates whether a sync is present between the source connected to the HDMI input and the receiver
- **Resolution:** The resolution of the source connected to the HDMI input
- **Source HDCP:** Indicates whether HDCP is active or inactive

Select **+ More Details** at the bottom of the tab to display an expanded section that shows additional information. Select **- More Details** to collapse the section.

HDMI Output

Select **HDMI Output** to view the status of a display device connected to the HDMI output.

Status – HDMI Output

▼ HDMI Output

– Connected Display

Sink Connected Yes

Manufacturer ACI

Name VE248

– Output Signal

Resolution 1920x1080@60

Disabled by HDCP No

+ More Details

Select the + (plus) icon next to **Connected Display** to view the following display settings:

- **Sink Connected:** Reports whether or not a display is connected
- **Manufacturer:** The manufacturer name of the display device
- **Name:** The name of the display device

Select the + (plus) icon next to **Output Signal** to view the following output signal settings:

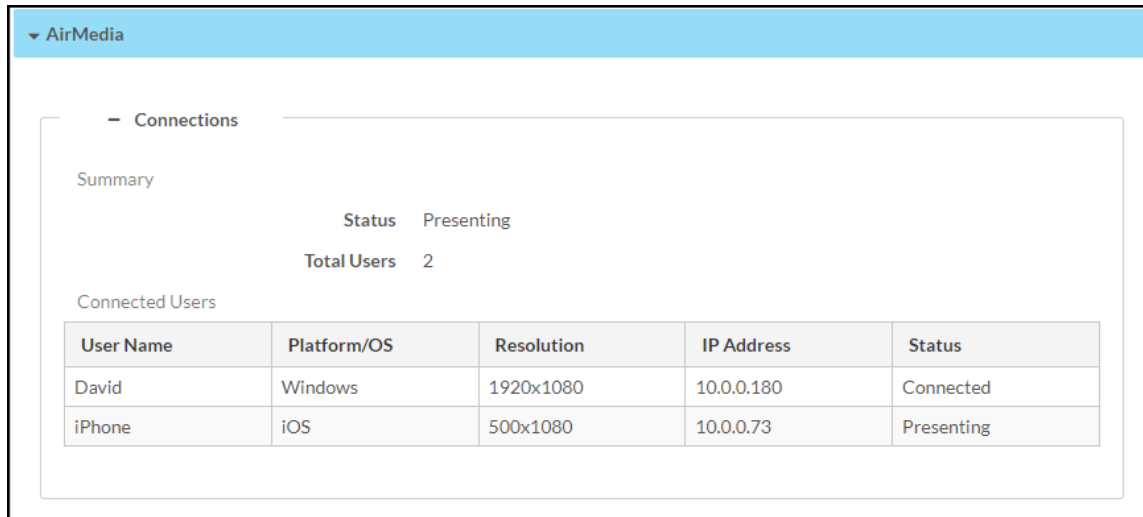
- **Resolution:** The resolution and frame rate of the display device
- **Disabled by HDCP:** Reports whether or not the display signal is disabled by HDCP

Select + **More Details** at the bottom of the tab to display an expanded section that shows additional information. Select - **More Details** to collapse the section.

AirMedia

Select **AirMedia** to view the status of the AirMedia connection.

Status – AirMedia Connection



The screenshot shows a web interface for AirMedia status. At the top is a blue header with a dropdown arrow and the text 'AirMedia'. Below this is a section titled 'Connections' with a minus icon. Inside this section, there is a 'Summary' area with 'Status' set to 'Presenting' and 'Total Users' set to '2'. Below the summary is a 'Connected Users' section containing a table with two rows of user data.

User Name	Platform/OS	Resolution	IP Address	Status
David	Windows	1920x1080	10.0.0.180	Connected
iPhone	iOS	500x1080	10.0.0.73	Presenting

Select the + (plus) icon next to **Connections** to view the connection settings for devices using AirMedia:

- **Summary:** Reports the status of the device and the total amount of users connected to the receiver
 - **Status:** Reports **Idle** when no users are connected, **Active** when a user is connected but not presenting, and **Presenting** when a user is presenting
 - **Total Users:** The total amount of users with an active connection to the receiver. The receiver supports a maximum of ten simultaneous connections and up to two simultaneous presenters.
- **Connected Users:** Reports the details of all users with an active connection to the device
 - **User Name:** The user name of a connected user
 - **Platform/OS:** The operating system of a connected device
 - **Resolution:** The resolution of a connected device
 - **IP Address:** The IP address of a connected device
 - **Status:** Reports **Idle** when no users are connected, **Active** when the user is connected but not presenting, and **Presenting** when the user is presenting

Control System

Select **Control System** to view the status of the receiver's control system connection.

Status – Control System

▼ Control System

Encrypt Connection OFF

– IP Table

IP ID	Room ID	IP Address/Hostname	Type	Server Port	Connection	Status
No records found						

The following **Control System** information is displayed:

- **Encrypt Connection:** Indicates whether the connection between the control system and the receiver is encrypted
- **IP Table:** Displays the IP table information for the control system connection:
 - **IP ID:** The IP ID used to connect the receiver to a control system
 - **Room ID:** The control system room ID that the receiver is associated with (for connections to the Crestron Virtual Control server-based control system)
 - **IP Address/Hostname:** The control system IP address or hostname
 - **Type:** The control system type
 - **Server Port:** The control system server port
 - **Connection:** The control system connection type
 - **Status:** The control system connection status

Connected Devices

Select **Connected Devices** to view the status of any connected devices such as a display, occupancy sensor, or touch panel.

Select the + (plus) icon next to **Connected Display** to view the following display settings:

Status – Connected Devices (Connected Display)

- Connected Display	
Manufacturer	ACI
Name	Display

- **Detected Manufacturer:** The manufacturer of the connected display
- **Detected Name:** The name given to the connected display

Select the + (plus) icon next to **Network Occupancy Sensor** to view the following occupancy sensor settings:

Status – Connected Devices (Network Occupancy Sensor)

- Network Occupancy Sensor	
Connection Status	NA
Occupancy Status	NA

- **Connection Status:** The occupancy sensor connection status
- **Occupancy Status:** The occupancy status (either **Occupied** or **Vacant**) of the space monitored by an occupancy sensor

Select the + (plus) icon next to **Touch Panel** to view the following touch panel settings:

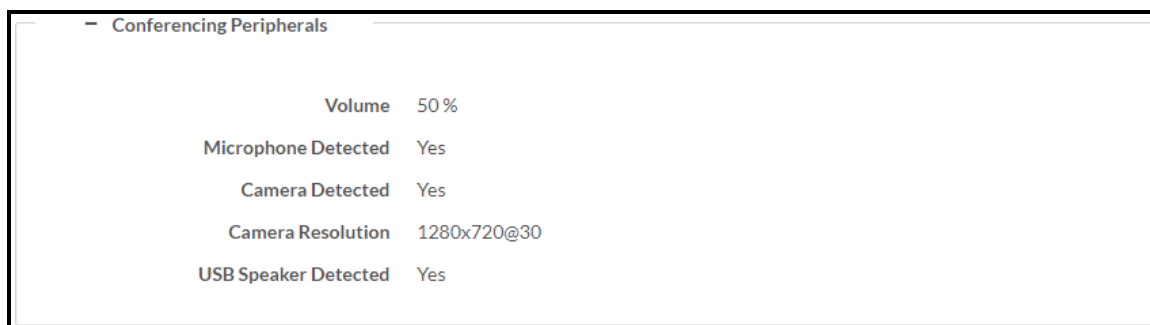
Status – Connected Devices (Touch Panel)

- Touch Panel	
Connection Status	NA
Model	TSW-1070

- **Connection Status:** The touch panel connection status
- **Model:** The model name of the touch panel

Select the + (plus) icon next to **Conferencing Peripherals** to view the following settings:

Status – Conferencing Peripherals



Volume	50 %
Microphone Detected	Yes
Camera Detected	Yes
Camera Resolution	1280x720@30
USB Speaker Detected	Yes

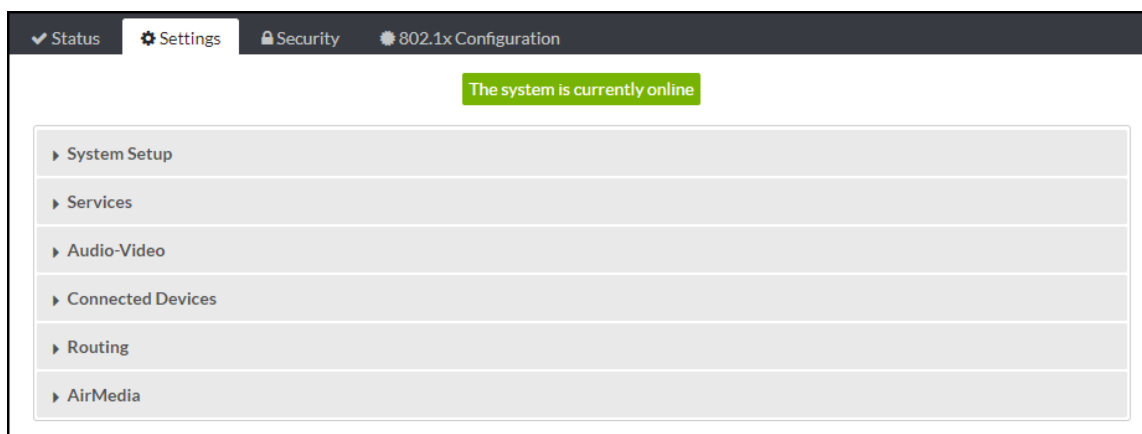
- **Volume:** The maximum allowed volume of connected USB speakers.
- **Microphone Detected:** Indicates whether or not a microphone is connected
- **Camera Detected:** Indicates whether or not a camera is connected
- **Camera Resolution:** The resolution of a connected camera
- **USB Speaker Detected:** Indicates whether or not a USB speaker is connected

Settings

Select **Settings** to configure various device settings. Once any changes have been made to the receiver configuration, the **Action** button becomes a **Save Changes** button. Select **Save Changes** to save changes to the configuration settings. If a reboot is required after changes have been saved, select **Yes** to reboot the device or **No** to cancel the reboot.

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

Settings Screen



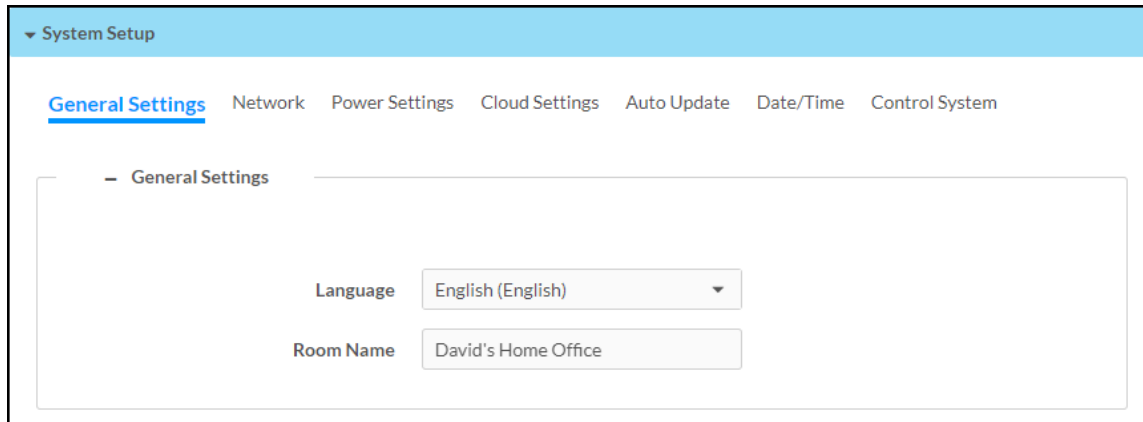
System Setup

Select **System Setup** to modify general, network, power, cloud, update, date/time, and control system settings.

General Settings

Select **General Settings** to configure general device settings.

System Setup – General Settings



The screenshot shows a web interface for 'System Setup'. At the top, there is a light blue header bar with a dropdown arrow and the text 'System Setup'. Below this, a horizontal navigation bar contains several tabs: 'General Settings' (which is underlined in blue), 'Network', 'Power Settings', 'Cloud Settings', 'Auto Update', 'Date/Time', and 'Control System'. The main content area is titled 'General Settings' with a minus sign icon. It contains two settings: 'Language' with a dropdown menu showing 'English (English)' and a downward arrow, and 'Room Name' with a text input field containing 'David's Home Office'.

- **Language:** Select the language that will be displayed on the receiver from the drop-down list
- **Room Name:** Enter the room name for the space that the receiver is installed in

Network

Select **Network** to configure the receiver's network settings.

System Setup – Network

System Setup

General Settings **Network** Power Settings Cloud Settings Auto Update Date/Time Control System

Network

Hostname

AM-3200-7D60-B-5050

Domain

hsd1.nj.comcast.net

SSH

☒

Primary Static DNS

Secondary Static DNS

Network Adapter 1 - Main

DHCP

☒

IP Address

10.0.0.238

Subnet Mask

255.255.255.0

Default Gateway

10.0.0.1

Network Adapter 2 - AUX

DHCP

☒

IP Address *

192.168.0.101

Subnet Mask *

255.255.255.0

Default Gateway *

192.168.0.1

Wireless Access Point

Wireless Access Point Mode

☐

Name/SSID

AM-3100-WF-ed7a6c

Security Key

Security

WPA2

Auto Launch AirMedia Landing Page

☐

WiFi Mode

5GHz Only

2.4GHz Channel

0

5GHz Channel

0 (Auto)

2.4GHz Signal Strength

100 %

5GHz Signal Strength

100 %

Network Proxy Settings

Proxy

☐

HTTP Settings

HTTP Proxy

☐

HTTP Proxy Address

HTTP Proxy Port

0

Username

Password

HTTPS Settings

HTTPS Proxy

☐

HTTPS Proxy Address

HTTPS Proxy Port

0

Username

Password

- **Host Name:** Enter the receiver host name (22 characters or less).
- **Domain:** Enter the fully qualified domain name on the network (optional). This field is prefilled when the **DHCP** toggle is turned on.

NOTE: A host name and domain name can act as an alternative to IP addressing for connecting client computers to the device.

- **SSH:** Turn on the toggle to enable Secure Shell protocol (SSH).
- **Primary Static DNS:** Enter the primary DNS address.
- **Secondary Static DNS:** Enter the secondary DNS address.
- **Network Adapter 1 - Main and Network Adapter 2 - AUX**

NOTE: Network Adapter 2 - AUX settings are unavailable on AM-3100-WF(-I) models.

- **DHCP:** Turn on the toggle to use DHCP for the Ethernet connection. When enabled, the IP address, subnet mask, and default gateway settings are automatically filled. If the toggle is off, these settings must be entered manually.
- **IP Address:** Enter the receiver IP address on the network. This field is prefilled when the DHCP toggle is on.
- **Subnet Mask:** Enter the device subnet mask address on the network. This field is prefilled when the DHCP toggle is on.
- **Default Gateway:** Enter the gateway router address on the network. This field is prefilled when the DHCP toggle is on.

- **Wireless Access Point:** The device can be used as a Wireless Access Point (WAP) so that users can present wirelessly without using a corporate Wi-Fi network.

NOTE: Wireless Access Point functionality is not available on the AM-3200. It is only available on Wi-Fi network capable AirMedia receivers.

- **Wireless Access Point Mode:** Turn on the toggle to enable the receiver to operate as a Wireless Access Point
- **Name/SSID:** Enter a name for the wireless network.
- **Security Key:** Enter a security key to connect to the wireless network.

NOTE: The wireless network name and security should each be 22 characters or fewer for optimal presentation on a display device and/or a connected touch screen.

- **Security:** Select an encryption key type to be used by the wireless network.

NOTE: When WPA2 is selected, WPA2-PSK is used by default for security key encryption.

- **Auto Launch AirMedia Landing Page:** Turn on the toggle to automatically launch a web browser and redirect the user to the AirMedia landing page upon connection to the wireless access point.
- **WiFi Mode:** Select **2.4GHz Only** or **5GHz Only** from the dropdown list to use either a 2.4GHz or 5GHz frequency band. Select **Concurrent** to use dual-band frequencies.
- **2.4GHz Channel:** Select the channel number. If **5GHz Only** is selected in the **WiFi Mode** field, then this field will not be editable.
- **5GHz Channel:** Select the channel number. If **2.4GHz Only** is selected in the **WiFi Mode** field, then this field will not be editable.

NOTE: Set either channel to **0 (Auto)** to enable automatic channel selection.

- **2.4GHz Signal Strength:** Select the signal strength for the 2.4GHz frequency band. If **5GHz Only** or **Concurrent** is selected in the **WiFi Mode** dropdown list, then the signal strength for the 2.4GHz band will automatically be set to 0.
- **5GHz Signal Strength:** Select the signal strength for the 2.4GHz frequency band. If **2.4GHz Only** or **Concurrent** is selected in the **WiFi Mode** dropdown list, then the signal strength for the 5GHz band will automatically be set to 0.

- **Network Proxy Settings**

- **Proxy:** Turn on the toggle to configure the device for use with a proxy server.

- **HTTP Settings**
 - **HTTP Proxy:** Turn on the toggle to allow the device to use an HTTP proxy server.
 - **HTTP Proxy Address:** Enter the IP address or the FQDN of the HTTP proxy server.
 - **HTTP Proxy Port:** Enter the port number of the HTTP proxy server.
 - **Username:** Enter the username required for the HTTP proxy server.
 - **Password:** Enter the password required for the HTTP proxy server.
- **HTTPS Settings**
 - **HTTPS Proxy:** Turn on the toggle to allow the device to use an HTTPS proxy server.
 - **HTTPS Proxy Address:** Enter the IP address or the FQDN of the HTTPS proxy server.
 - **HTTPS Proxy Port:** Enter the port number of the HTTPS proxy server.
 - **Username:** Enter the username required for the HTTPS proxy server.
 - **Password:** Enter the password required for the HTTPS proxy server.

Power Settings

Select **Power Settings** to configure the receiver's power settings.

System Setup - Power Settings

System Setup

General Settings Network **Power Settings** Cloud Settings Auto Update Date/Time Control System

Power Settings

Power Mode Business Hours + Occupancy ... ⓘ

Enabled	Day	On Time	Off Time
☒	Sunday	00:00	23:59
☒	Monday	00:00	23:59
☒	Tuesday	00:00	23:59
☒	Wednesday	00:00	23:59
☒	Thursday	00:00	23:59
☒	Friday	00:00	23:59
☒	Saturday	00:00	23:59

The **Power Mode** setting allows the receiver to go to sleep based on business hours and/or room occupancy.

Select a **Power Mode** option from the dropdown list:

NOTE: Business Hours + Occupancy Based is the default setting.

- Select **Business Hours + Occupancy Based** to apply the following behavior:
 - The display device is on and the receiver is awake during business hours. Define business hours using the table:
 - **Enabled:** Turn the toggle on to include the day in the business hours schedule.
 - **On Time:** Enter the time of day (in 24-hour format) when business hours begin.
 - **Off time:** Enter the time of day (in 24-hour format) when business hours end.
- NOTE:** When the **On Time** and **Off Time** settings are set to **00:00** and **23:59** respectively, the display device is on and the receiver is awake all day.
- The touch screen is always on.
 - Crestron Fusion power events are ignored.
 - If room occupancy or vacancy is detected outside of business hours, the receiver wakes up or goes to sleep accordingly.
 - Virtual button power events are allowed.
 - If an HDMI sync is detected outside of business hours, the receiver wakes up.
- Select **Based on Occupancy** to apply the following behavior:
 - The connected occupancy sensor determines when the room is occupied or vacant.
 - If room vacancy is detected, the receiver goes to sleep.
 - If room occupancy is detected, the receiver wakes up.
 - If the display device is configured as a controlled display device, it powers on when the room is occupied and powers off when the room is vacant.
 - The touch screen is on when the room is occupied and off when the room is vacant.
 - Crestron Fusion power events are permitted.
 - If an HDMI sync is detected, the receiver wakes up.
 - An AirMedia connection does not wake the receiver.

- Select **Signage Only** to apply the following behavior:
 - All user presentation capabilities are disabled.
 - The display device and the receiver will always present digital signage during business hours and turn off outside of business hours. Define business hours using the table:
 - **Enabled:** Turn the toggle on to include the day in the business hours schedule.
 - **On Time:** Enter the time of day (in 24-hour format) when business hours begin.
 - **Off time:** Enter the time of day (in 24-hour format) when business hours end.

NOTE: When the **On Time** and **Off Time** settings are set to **00:00** and **23:59** respectively, the display device is on and the receiver is awake all day.

- The connected occupancy sensor determines when the room is occupied or vacant.
- If room occupancy is detected outside of business hours, the receiver and display device power on. Digital signage is displayed.
- If room vacancy is detected outside of business hours, the receiver and display device power off.
- The touch screen is always off.
- Crestron Fusion power events are permitted.

NOTE: To use the **Signage Only** power mode, enable the **Signage in Standby** setting as described in [Digital Signage](#).

- Select **Business Hours + Occupancy Based for Signage** to apply the following behavior:
 - The display device and the receiver will turn on during business hours and turn off outside of business hours. Define business hours using the table:
 - **Enabled:** Turn the toggle on to include the day in the business hours schedule.
 - **On Time:** Enter the time of day (in 24-hour format) when business hours begin.
 - **Off time:** Enter the time of day (in 24-hour format) when business hours end.

NOTE: When the **On Time** and **Off Time** settings are set to **00:00** and **23:59** respectively, the display device is on and the receiver is awake all day.

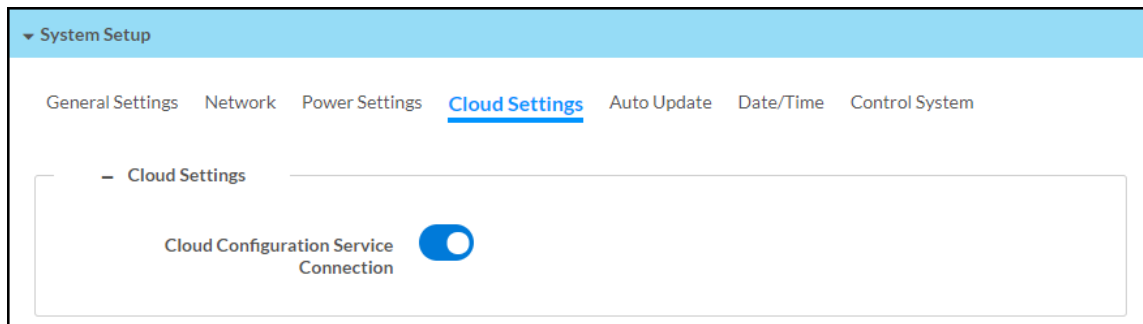
- The connected occupancy sensor determines when the room is occupied or vacant.
- If room vacancy is detected during business hours, the receiver goes to sleep. Digital signage is displayed.
- If room occupancy is detected during business hours, the receiver wakes up.
- If room vacancy is detected outside of business hours, the receiver and display device power off.
- If room occupancy is detected outside of business hours, the receiver and display device power on.
- The touch screen is on when the room is occupied and off when the room is vacant.
- Crestron Fusion power events are permitted.
- If an HDMI sync is detected, the receiver wakes up.
- An AirMedia connection does not wake the receiver.

NOTE: The **Business Hours + Occupancy Based With Signage** setting must be selected if Appspace is to be used.

Cloud Settings

Select **Cloud Settings** to configure the device's connection to the XiO Cloud® service. By default, the **Cloud Configuration Service Connection** toggle is turned on. For more information on using the XiO Cloud service with an AirMedia receiver, refer to [Enterprise Deployment Options \(on page 75\)](#).

System Setup - Cloud Settings

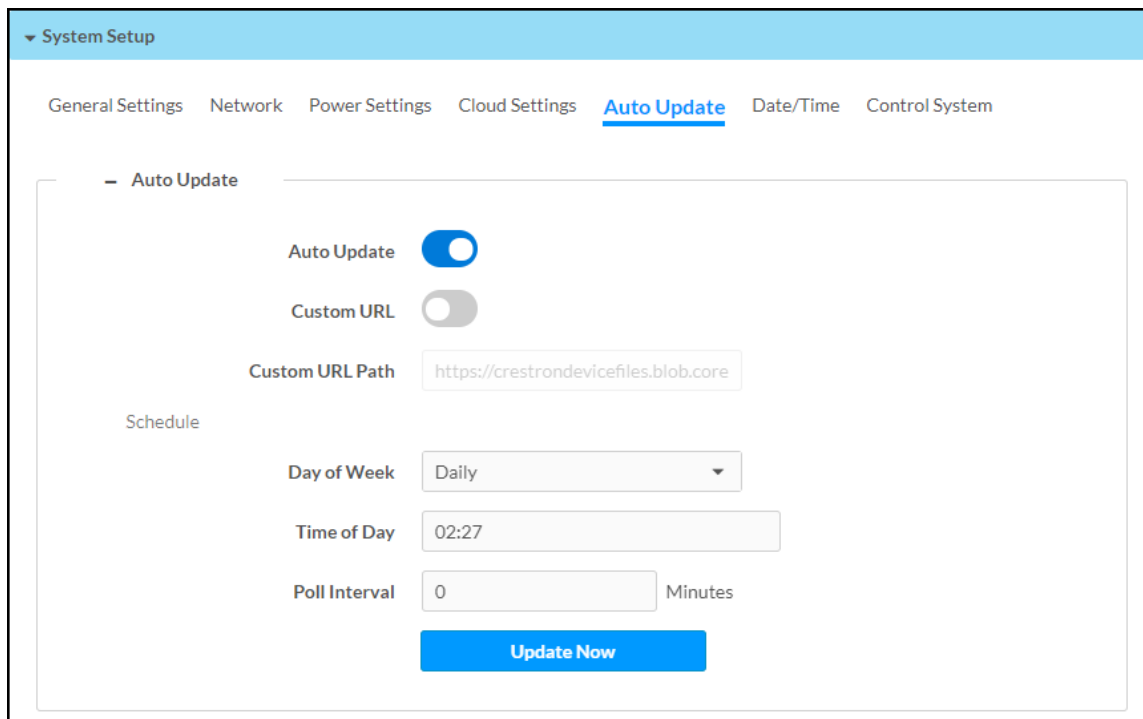


The screenshot shows the 'System Setup' menu with 'Cloud Settings' selected. The 'Cloud Configuration Service Connection' toggle is turned on.

Auto Update

Select **Auto Update** to configure the auto update feature. The auto update feature allows the device to automatically scan for firmware updates and install the updates as needed.

System Setup - Auto Update



The screenshot shows the 'System Setup' menu with 'Auto Update' selected. The 'Auto Update' toggle is turned on. The 'Custom URL' toggle is turned off. The 'Custom URL Path' is set to 'https://crestrondevicefiles.blob.core'. The 'Schedule' section shows 'Day of Week' set to 'Daily', 'Time of Day' set to '02:27', and 'Poll Interval' set to '0' minutes. An 'Update Now' button is at the bottom.

- **Auto Update:** Turn the toggle on to allow automatic updates.
- **Custom URL:** Turn the toggle on to use a custom update server URL. If turned off, the server URL will default to the standard Crestron update server.
- **Custom URL Path:** If **Custom URL** is turned on, enter the custom URL path for the update server.
- **Schedule:** Set the schedule for when the device checks for updates.
 - **Day of Week:** Select the day of the week when the device will check for updates. Select **Daily** to have the device check for updates every day.
 - **Time of Day:** Enter a time of day (in 24-hour format) when the device will check updates on the scheduled day.
 - **Poll Interval:** Enter the polling interval (in minutes) for when the device will poll the server for updates.
 - Select **Update Now** to check the update server for new firmware and to update the device immediately if new firmware is available.

Date/Time

Select **Date/Time** to configure the settings for the receiver's internal clock.

System Setup – Configure Date/Time

The screenshot shows the 'Date/Time' configuration page within the 'System Setup' menu. The page has a light blue header with the title 'System Setup' and a navigation bar with links: General Settings, Network, Power Settings, Cloud Settings, Auto Update, **Date/Time** (highlighted), and Control System. Below the navigation bar, the 'Date/Time' section is expanded, showing a 'Synchronization' toggle for 'Time Synchronization' which is turned on. A blue 'Synchronize Now' button is located below the toggle. Under the 'NTP Time Servers' section, there is a table with columns: Address, Port, Authentication Method, Authentication Key, and Key ID. One server is listed with Address 'pool.ntp.org', Port '123', Authentication Method 'None', Authentication Key '.....', and Key ID '0'. Below the table are '+ Add' and '- Remove' buttons. The 'Configuration' section at the bottom includes dropdowns for 'Time Zone' (set to '(UTC - 05: 00) Eastern Time (US & ...)', 'Date Format' (set to 'MDY'), and 'Time Format' (set to '12'). It also has input fields for 'Date' (07/28/2021) and 'Time' (09:06).

▼ System Setup

General Settings Network Power Settings Cloud Settings Auto Update **Date/Time** Control System

– Date/Time

Synchronization

Time Synchronization ☒

Synchronize Now

NTP Time Servers

☐	Address	Port	Authentication Method	Authentication Key	Key ID
☐	pool.ntp.org	123	None		0

+ Add – Remove

Configuration

Time Zone (UTC - 05: 00) Eastern Time (US & ...)

Date Format MDY

Time Format 12

Date 07/28/2021

Time 09:06

- **Synchronization:** The receiver's internal clock can be synchronized with a time server.
 - **Time Synchronization:** Turn on the toggle to use time synchronization via SNTP (Simple Network Time Protocol).
 - **Synchronize Now:** With **Time Synchronization** turned on, select **Synchronize Now** to synchronize the receiver with the SNTP server(s) entered in the **NTP Time Servers** table.

- **NTP Time Servers:** With **Time Synchronization** turned on, use the provided table to enter information regarding the SNTP server(s) used to synchronize the date and time for the receiver.
 - 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** dropdown 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 checkbox to the left of the table entry, and then select **Remove**.
- **Configuration:** The receiver's internal clock can be configured manually.
 - **Time Zone:** Select a time zone for the receiver using the dropdown menu.
 - **Date Format:** Select the format that the date will appear on the display device using the drop-down menu (**MDY**, **DMY**, or **YMD**).
 - **Time Format:** Select the format that the time will appear on the display device (12 hour or 24 hour).
 - **Date:** Select the date for the receiver using the pop-up calendar that is displayed.

Control System

Select **Control System** to connect and configure a control system with the receiver. The receiver can be controlled by a Crestron control system or by a virtual control system's SIMPL or SIMPL# program.

System Setup – Control System

System Setup

General Settings Network Power Settings Cloud Settings Auto Update Date/Time Control System

Control System

Encrypt Connection ☒

Control System Username

Control System Password

IP Table

☐	IP ID	IP Address/Hostname	Room ID
No records found			
+ Add x Remove			

- **Encrypt Connection:** Turn the toggle on to use SSL encryption for communication with the control system. SSL can be used with or without a CA certificate. When **Encrypt Connection** is toggled on, the username and password for the control system is required.
- **Control System Username:** The username for the control system.
- **Control System Password:** The password for the control system.
- **IP Table:** Select **Add** to add an IP table connection between the device and the control system.
 - **IP ID:** Enter an IP ID for connecting the device to the control system.

NOTES:

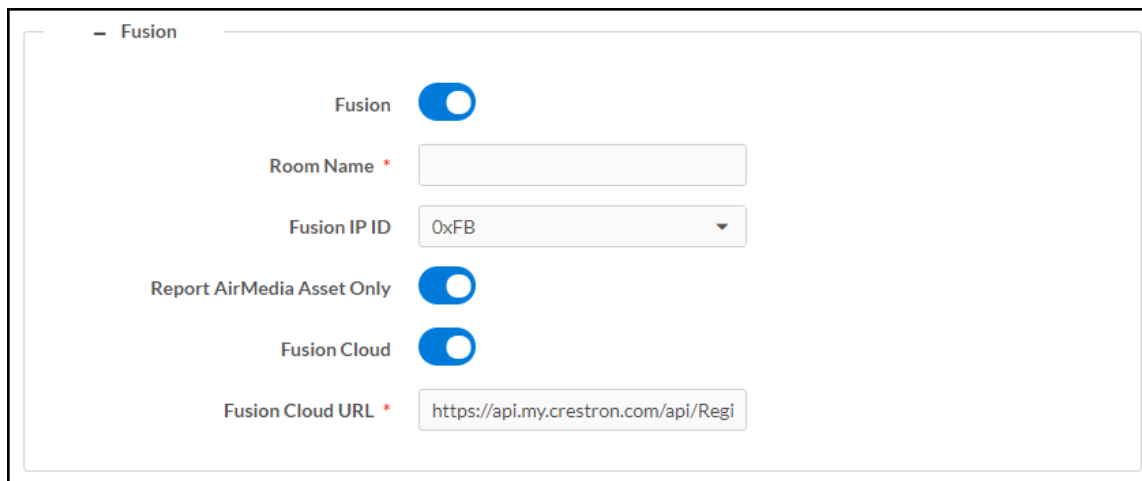
- The control system will search the related ID while entering the IP ID.
 - The IP ID must match the IP ID defined in the control system's SIMPL Windows or SIMPL# program.
- **IP Address/Hostname:** Enter the control system IP address or hostname.
 - **Room ID:** Enter a room ID to associate with the device (for connections with the Crestron Virtual Control server-based control system).

Services

Select **Services** to configure the device's connection with Crestron Fusion® software and/or other calendaring applications.

At the top left corner of the **Services** window, select the + (plus) icon next to **Fusion** to configure the following Crestron Fusion connection settings.

Settings Tab - Services (Fusion)

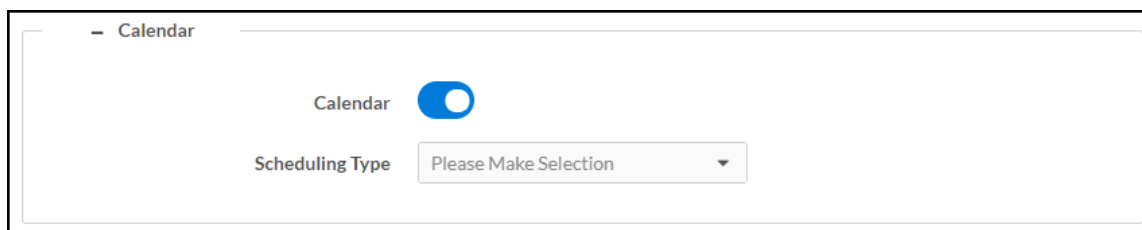


- **Fusion:** Turn the toggle on to use Crestron Fusion with the device.
- **Room Name:** Enter the room name to be used by the Crestron Fusion server.
- **Fusion IP ID:** Select the IP ID number to be used by the Crestron Fusion server.
- **Report AirMedia Asset Only:** Turn the toggle on to allow only AirMedia related settings to appear in Crestron Fusion. Turn the toggle off to allow all device settings to appear in Crestron Fusion.
- **Fusion Cloud:** Turn the toggle on and enter the Fusion Cloud URL manually in the **Fusion Cloud URL** field. When **Fusion Cloud** is toggled off, the Crestron Fusion server will use auto-discovery and the **Fusion Cloud URL** field will not appear.

NOTE: Upon completion, the device will be brought into Crestron Fusion software as a processor. For more details on using the device with Crestron Fusion, refer to the Crestron Fusion help file.

Select the + (plus) icon next to **Calendar** to display the following calendaring application settings.

Settings Tab - Services (Calendar)



The screenshot shows a settings window titled "Calendar". Inside, there is a toggle switch labeled "Calendar" which is currently turned on (blue). Below it, there is a label "Scheduling Type" followed by a dropdown menu that currently displays "Please Make Selection".

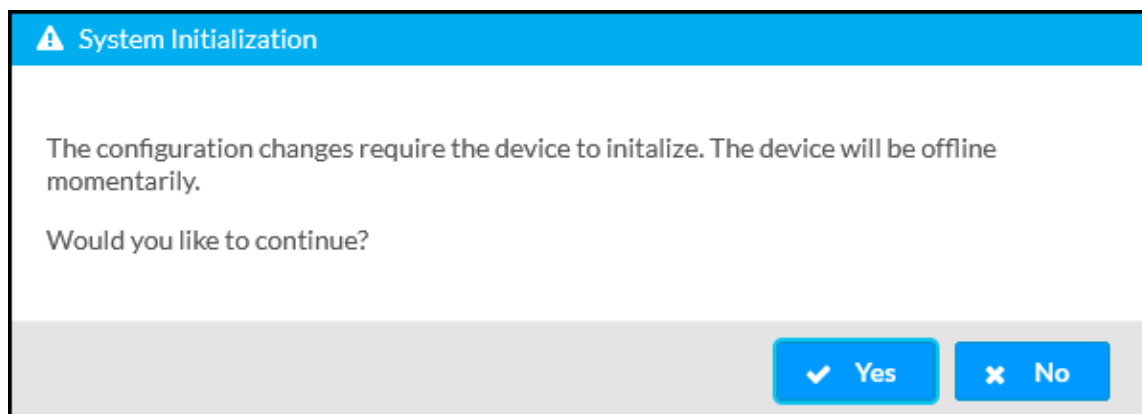
- **Calendar:** Turn the toggle on to use a calendaring application with the AirMedia device.
- **Scheduling Type:** Select a calendaring service from the dropdown menu.

Crestron Fusion Service

To use the device with Crestron Fusion scheduling software:

1. Configure a Crestron Fusion connection as described in [Services \(on the previous page\)](#).
2. Turn on the **Calendar** toggle.
3. Select **Fusion** from the **Scheduling Type** drop-down menu.
4. Select **Save Changes**. In the **System Initialization** dialog box, select **Yes** to continue. System initialization will occur.

System Initialization



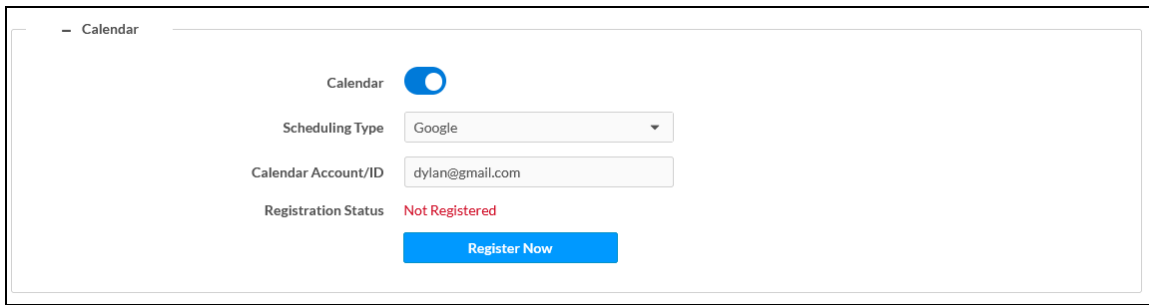
The screenshot shows a "System Initialization" dialog box. It has a blue header bar with a warning icon and the text "System Initialization". The main content area contains the text: "The configuration changes require the device to initialize. The device will be offline momentarily." followed by the question "Would you like to continue?". At the bottom right, there are two buttons: "Yes" with a checkmark icon and "No" with an "x" icon.

Google Calendar Service

To use the device with the Google Calendar service:

1. Turn on the **Calendar** toggle as described in [Services \(on the previous page\)](#).
2. Select **Google** from the **Scheduling Type** drop-down list to use the Google Calendar™ application for calendar functions.

Calendar Settings – Google Calendar



Calendar ☒

Scheduling Type Google

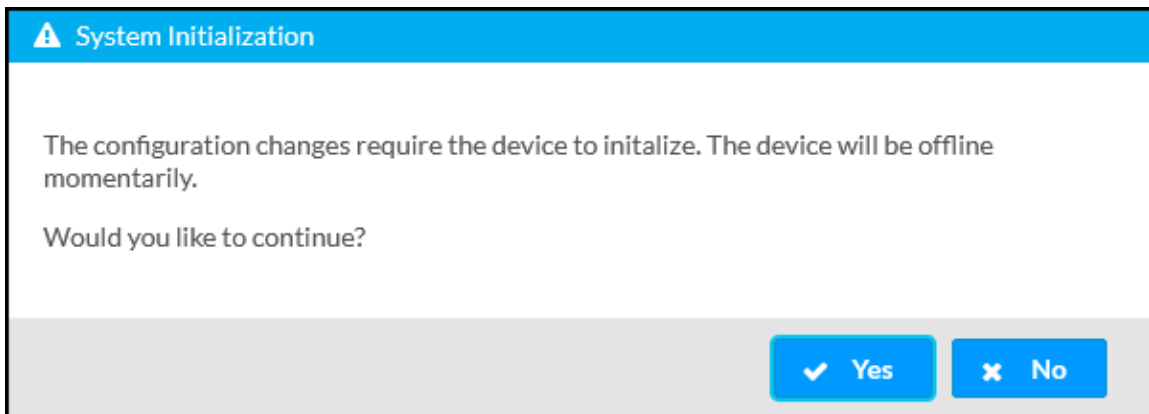
Calendar Account/ID dylan@gmail.com

Registration Status Not Registered

[Register Now](#)

3. In the **Calendar Account/ID** field, enter the email address attached to the desired Google calendar.
4. Select **Save Changes**. In the **System Initialization** dialog box, select **Yes** to continue. System initialization will occur.

System Initialization



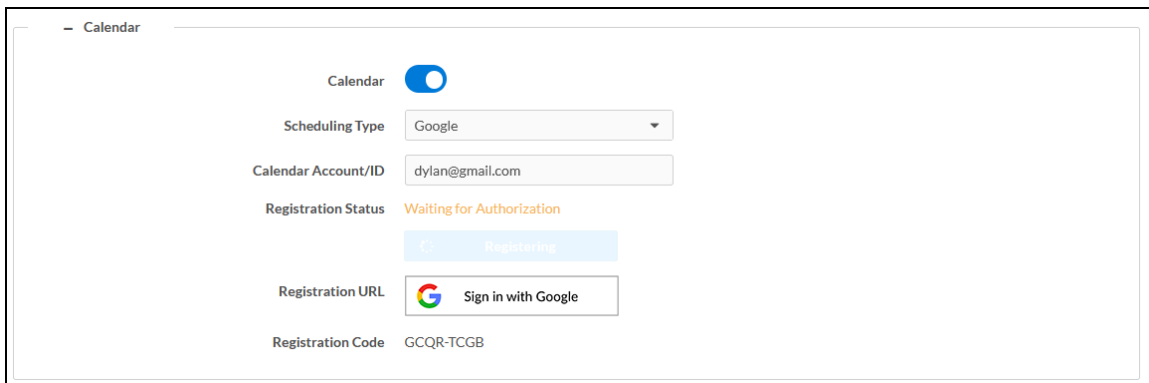
System Initialization

The configuration changes require the device to initialize. The device will be offline momentarily.

Would you like to continue?

[Yes](#) [No](#)

5. Select **Register Now**. The **Registration Status**, **Registration URL**, and **Registration Code** fields will appear.



Calendar ☒

Scheduling Type Google

Calendar Account/ID dylan@gmail.com

Registration Status Waiting for Authorization

[Registering](#)

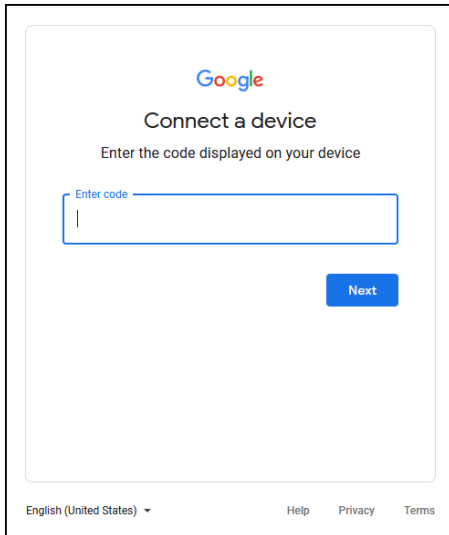
Registration URL  Sign in with Google

Registration Code GCQR-TCGB

6. Copy the code in the **Registration Code** field.

7. In the **Registration URL** field, select **Sign in with Google**. The **Connect a device** screen appears.

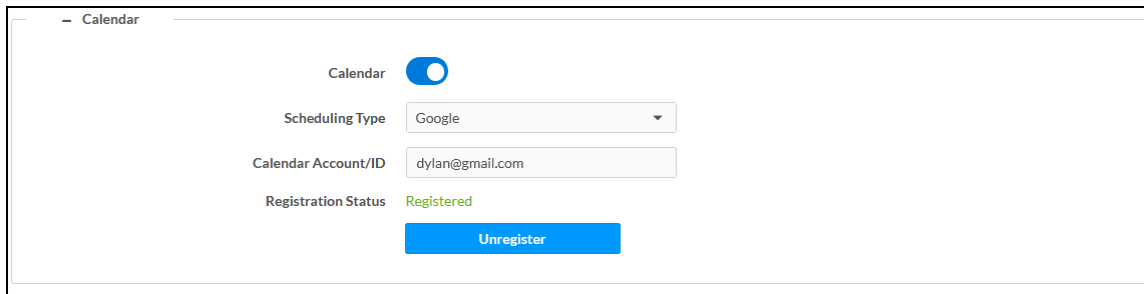
Connect a device Screen

The image shows a web interface for connecting a device. At the top is the Google logo. Below it, the heading "Connect a device" is centered, followed by the instruction "Enter the code displayed on your device". There is a text input field with the placeholder "Enter code" and a blue "Next" button to its right. At the bottom of the interface, there is a language selector set to "English (United States)" and links for "Help", "Privacy", and "Terms".

8. Enter the registration code in the **Enter Code** field and select **Next**. The **Choose an account** screen appears.
9. Select an account and sign in with the login credentials.
10. Select **Allow** to complete the process. A success message will be displayed, and the Google Calendar status will be updated.

To disconnect the calendar from the device, select **Unregister** and follow the instructions for activating a new configuration.

Calendar Settings – Google Calendar

The image shows a settings page titled "Calendar". At the top, there is a toggle switch for "Calendar" which is turned on. Below this, there are three settings: "Scheduling Type" is set to "Google" in a dropdown menu; "Calendar Account/ID" is set to "dylan@gmail.com" in a text field; and "Registration Status" is "Registered" in green text. At the bottom, there is a blue "Unregister" button.

Microsoft Exchange Server and Microsoft 365 Software, Modern Authentication

To use the device with Microsoft Exchange Server and Microsoft 365 Software (Modern Authentication enabled):

1. Turn on the **Calendar** toggle as described in [Services \(on page 38\)](#).
2. Select **Exchange/O365** from the **Scheduling Type** dropdown menu.
3. Turn on the **Enable Modern Authentication** toggle.
4. Enter a Client ID in the **Client ID (Application ID)** field.
5. Enter an O365/Microsoft 365 Tenant ID in the **O365 Tenant ID** field.
6. (Optional) Enter the Calendar email address in the **Calendar Email Address** field. The calendar email address is required for accounts using impersonation.

Services – Calendar

Calendar ☒

Scheduling Type Exchange/O365 ▼

Enable Modern Authentication ☒

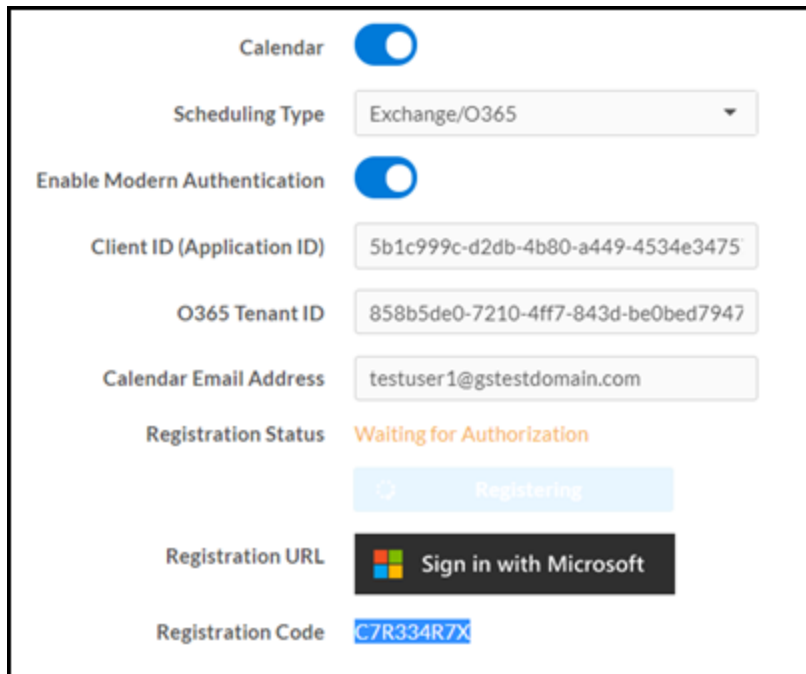
Client ID (Application ID) 3aaf74-a815-4975-86d3-b722094438e1

O365 Tenant ID 3b5de0-7210-4ff7-843d-be0bed794735

Calendar Email Address testuser1@gstestdomain.com

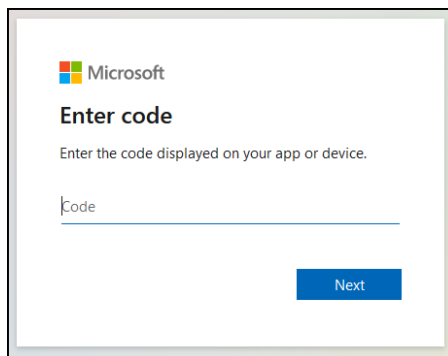
7. Select **Save Changes**. In the **System Initialization** dialog box, select **Yes** to continue. System initialization will occur.

8. Select **Register Now**. A code and a Microsoft icon will appear.



The screenshot shows a registration configuration interface. At the top, there is a 'Calendar' toggle switch which is turned on. Below it is a 'Scheduling Type' dropdown menu set to 'Exchange/O365'. Further down is an 'Enable Modern Authentication' toggle switch, also turned on. The 'Client ID (Application ID)' field contains the value '5b1c999c-d2db-4b80-a449-4534e3475'. The 'O365 Tenant ID' field contains '858b5de0-7210-4ff7-843d-be0bed7947'. The 'Calendar Email Address' field contains 'testuser1@gstestdomain.com'. The 'Registration Status' is indicated as 'Waiting for Authorization' in orange text. Below this status is a light blue button with a circular arrow icon and the text 'Registering'. The 'Registration URL' field displays a dark button with the Microsoft logo and the text 'Sign in with Microsoft'. Finally, the 'Registration Code' field shows the code 'C7R334R7X' in blue text.

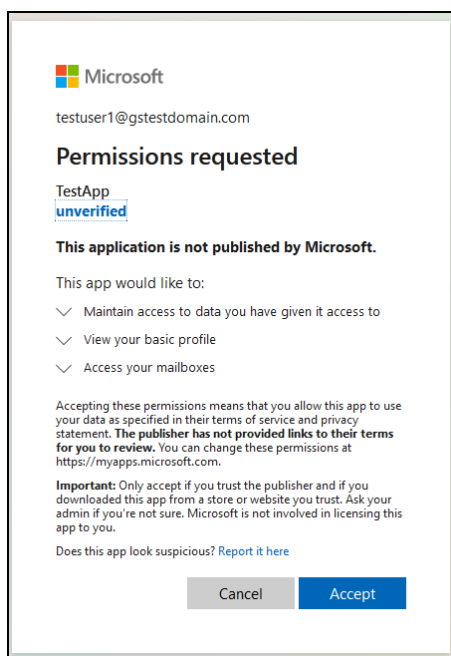
9. Copy the code in the **Registration Code** field.
10. Select **Sign in with Microsoft** in the **Registration URL** field. An **Enter code** screen will appear.



The screenshot shows a Microsoft 'Enter code' screen. At the top left is the Microsoft logo. Below it, the text 'Enter code' is displayed, followed by the instruction 'Enter the code displayed on your app or device.' There is a text input field with the placeholder text 'Code'. At the bottom right of the screen is a blue button labeled 'Next'.

11. Enter the registration code and select **Next**.
12. Enter the account credentials to sign in.

13. On first use, a permissions required window will be displayed. Select **Accept**.



14. Sign in to the Microsoft 365 service. Once signed in, a confirmation message will appear, and the Registration Status will be updated.

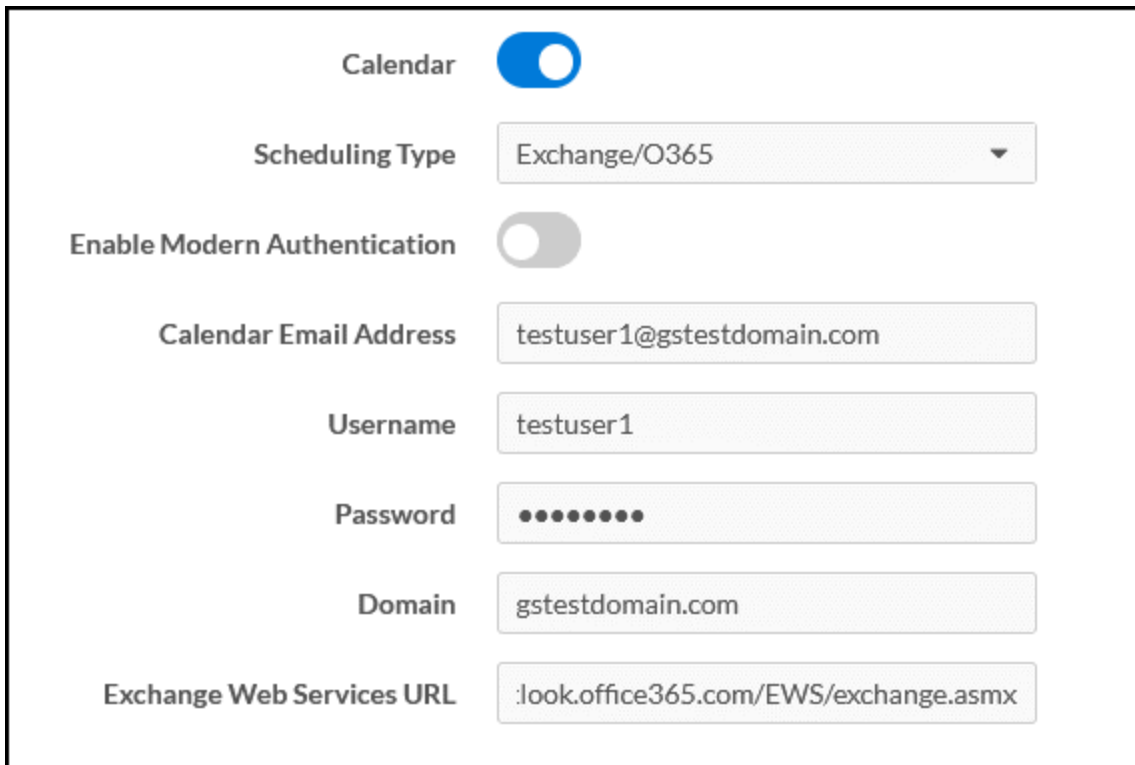
To disconnect the calendar from the device, select **Unregister** and follow the instructions for activating a new configuration.

Microsoft Exchange Server and Microsoft 365 Software, Modern Authentication Disabled

To use the device with Microsoft Exchange Server and Microsoft 365 Software (Modern Authentication disabled):

1. Turn on the **Calendar** toggle as described in [Services \(on page 38\)](#).
2. Select **Exchange/O365** from the **Scheduling Type** drop-down menu.
3. Turn the **Enable Modern Authentication** toggle off.
4. (Optional) Enter the calendar email address in the **Calendar Email Address** field. The calendar email address is required for accounts using impersonation.
5. Enter the account username in the **Username** field.
6. Enter the account password in the **Password** field.
7. Enter the domain name used by the Exchange server in the **Domain** field.

8. Enter the URL of the Exchange server in the **Exchange Web Services URL** field.



The screenshot shows a configuration window for Exchange Web Services. It includes a 'Calendar' toggle switch that is turned on. Below it is a 'Scheduling Type' dropdown menu set to 'Exchange/O365'. There is an 'Enable Modern Authentication' toggle switch that is turned off. The 'Calendar Email Address' field contains 'testuser1@gstestdomain.com'. The 'Username' field contains 'testuser1'. The 'Password' field is masked with dots. The 'Domain' field contains 'gstestdomain.com'. The 'Exchange Web Services URL' field contains ':look.office365.com/EWS/exchange.asmx'.

9. Select **Save Changes**. In the **System Initialization** dialog box, select **Yes** to continue. System initialization will occur.

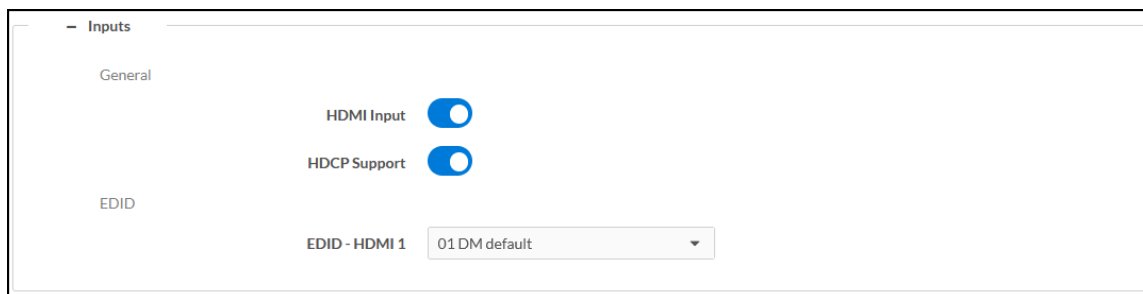
To disconnect the calendar from the device, select **Unregister** and follow the instructions for activating a new configuration.

Audio-Video

Select **Audio-Video** to configure settings for the HDMI input port (AM-3200(-WF)(-I) models only) and HDMI output port and to display information about the display device and output signal.

Select the **+** (plus) icon next to **Inputs** to display the following HDMI input settings.

Settings Tab - Audio-Video (Inputs)



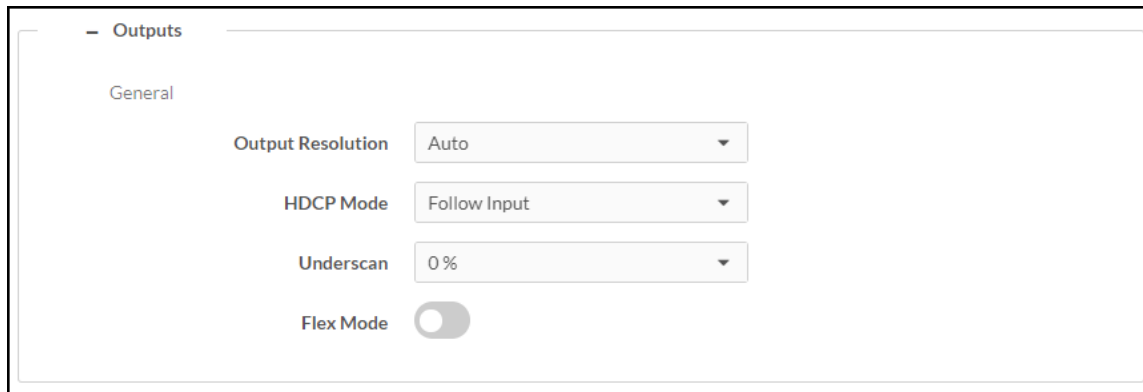
The screenshot shows the 'Inputs' settings tab. It has a 'General' section with 'HDMI Input' and 'HDCP Support' toggle switches, both of which are turned on. There is an 'EDID' section with 'EDID - HDMI 1' and a dropdown menu set to '01 DM default'.

- **General**
 - **HDMI Input:** Turn the toggle on to enable the HDMI input port.
 - **HDCP Support:** Turn the toggle on to allow source signals that require HDCP compliance to pass through to the display device.
- **EDID**
 - **EDID-HDMI 1:** Select an EDID profile loaded to the receiver to use for the HDMI input.

NOTE: To manage EDID profiles installed on the receiver, refer to [Manage EDIDs \(AM-3200\(-WF\)\(-I\) Models Only\) \(on page 10\)](#).

Select the + (plus) icon next to **Outputs** to display the following HDMI output settings.

Settings Tab - Audio-Video (Outputs)



The screenshot shows the 'Outputs' settings page. At the top, there is a minus icon and the label 'Outputs'. Below this is the 'General' section. It contains four settings: 'Output Resolution' set to 'Auto', 'HDCP Mode' set to 'Follow Input', 'Underscan' set to '0%', and 'Flex Mode' which is a toggle switch currently turned off.

- **Output Resolution:** Select the output resolution from the dropdown list.
- **HDCP Mode:** Select the HDCP mode from the dropdown list.
 - When **HDCP Mode** is set to **Auto**, the receiver always attempts to use HDCP if support is detected on the display device.
 - When **HDCP Mode** is set to **Follow Input**, the receiver attempts to use HDCP if support is detected on the HDMI input.
 - When **HDCP Mode** is set to **Force Highest**, the receiver attempts to use the latest version of HDCP regardless of whether or not support is detected on the display device.
 - When **HDCP Mode** is set to **Never Authenticate**, the receiver never attempts to use HDCP with downstream devices, regardless of support.
- **Underscan:** Select the amount of underscan to apply to the output signal from the dropdown list. Adjust this setting to improve the readability of text that may be cropped due to overscan or underscan conditions on the display device.

- **Flex Mode:** Turn the toggle on when using the receiver with a Crestron Flex conference system. Flex Mode disables the HDMI output from the AirMedia device unless a source is active.

NOTE: When using the device in Flex Mode, Crestron recommends setting **HDCP Mode** to **Never**. A connected touch screen must be set to communicate to the device at the IP ID FD. In **System Setup > Power Settings**, **Standby Mode** must be set to **Always On** as described in [Power Settings \(on page 29\)](#).

Connected Devices

Select **Connected Devices** to configure settings for any connected devices such as displays, touch screens, occupancy sensors and/or Wireless Conferencing peripherals.

Settings Screen - Connected Devices

Select the + (plus) icon next to **Connected Devices** to display the following device settings.

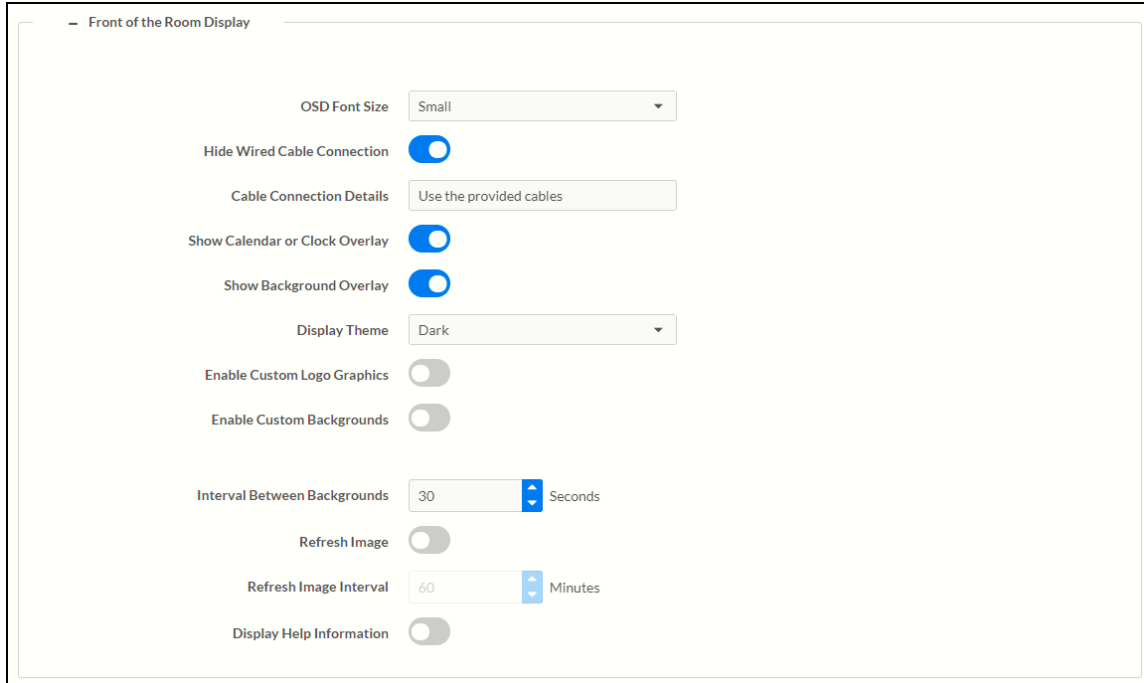
Settings Screen – Connected Devices (Connected Devices)

Connected Devices				
Name	Type ↕	Model	Status	Actions
POE Occupancy Sensor	Poe	CEN-ODT-C-POE	NA	 
Panel	Touch Panel	TSW-1070	NA	 
Display	Video Display	CEC Controlled-Display	NA	 

A list of connected devices is along with each device's **Name**, **Type**, **Model**, and **Status** . Select the edit button  to modify the connected device's settings. Select the test driver button  to send commands to a display device to test the driver's functionality.

Select the + (plus) icon next to **Front of the Room Display** to display settings for the front of the room experience splash screen.

Settings Screen – Connected Devices (Front of the Room Display)



- **OSD Font Size:** Select the font size of the connection bar text on the AirMedia Welcome Screen (**Small**, **Medium**, or **Large**).
- **Hide Wired Cable Connection:** (AM-3200(-WF)(-I) models only) Turn the toggle on to hide wired connection details on the display device.
- **Cable Connection Details:** (AM-3200(-WF)(-I) models only) Enter custom instructions for presenting content using the receiver's wired connection. The instructions will appear on the display device and should be used to guide users.
- **Show Calendar or Clock Overlay:** Turn the toggle on to show the clock and calendared events in the center of the display device.
- **Show Background Overlay:** Turn the toggle on to place a monochrome filter over background images.
- **Display Theme:** Select a display theme from the dropdown menu to use a light or dark color scheme on the display device.

- **Enable Custom Logo Graphics:** Turn the toggle on to display a custom logo on the display device. An **Add Logo** option will appear when the change is saved. When the toggle is off, the Crestron logo is displayed.

NOTES:

- The optimal image size for a logo is 600 x 100 pixels. Custom graphics that are larger than 600 x 100 pixels are scaled down while maintaining their aspect ratio. Custom graphics that are smaller than 600 x 100 pixels are not scaled up and should be resized for optimal image display.
- To manage images stored on the receiver, refer to [Manage Images \(on page 14\)](#). Up to 20 images can be stored locally on the receiver at a maximum of 100 MB.
- **Logo and Custom Background Management:** Select **Add Logo** to use a custom image. Choose an image located on a server or upload a custom image.
- **Source:** Select **URL** to use an image located on a server. Enter the URL of the image location in the **Graphic URL** field. Select **File** to upload an image file.
- **Enable Custom Backgrounds:** Turn the toggle on to display a custom background slideshow when the system is not in use. An **Add Logo** option will appear once the change is saved.

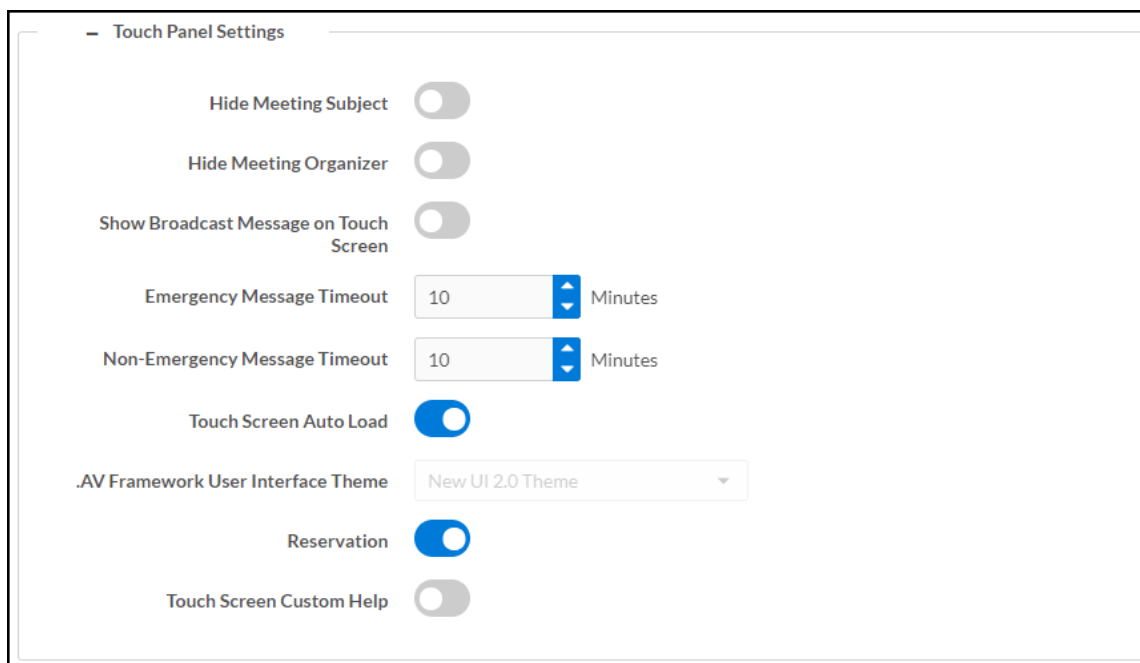
NOTES:

- Up to 20 images can be stored locally on the receiver at a maximum of 100 MB. To manage images stored on the receiver, refer to [Manage Images \(on page 14\)](#).
- Custom background images should be jpg files with resolutions no higher than 4096 x 2160 pixels. Images with resolutions higher than 4096 x 2160 pixels may exceed the receiver's storage limit when rendered and will inhibit performance.
- The interface has been designed to use most of the screen area for informational purposes. This feature is intended for use with corporate colors, branding, and aesthetics unique to the particular organization and should not be used to add custom instructions for room users.
- **Logo and Custom Background Management:** Select **Add Logo** to upload a custom image. Choose an image located on a server or upload a custom image.
- **Source:** Select **URL** to use an image located on a server. Enter the URL of the image location in the **Graphic URL** field. Select **File** to upload an image file. The image is then added to a list of files in the File drop-down menu. Select the image file from the dropdown menu.
- **Interval Between Backgrounds:** Enter a span of time (in seconds) that each background image is displayed.
- **Refresh Image:** Turn the toggle on to allow the system to periodically download the remotely stored logo and background images from the URLs specified for the custom logo or background.

- **Refresh Image Interval:** Enter the amount of time between downloads (in minutes). The minimum amount of time available is one minute, and the maximum amount of time is 65,535 minutes (about 45 days).
- **Display Help Information:** Turn the toggle on to allow the system to display custom help information. Enter the **Help Information Text** to be displayed.

Select the + (plus) icon next to **Touch Panel Settings** to display settings for connected touch screens.

Settings Screen – Connected Devices (Touch Panel Settings)



- **Hide Meeting Subject:** Turn the toggle on to hide the meeting's subject on the touch screen.
- **Hide Meeting Organizer:** Turn the toggle on to hide the meeting's organizer on the touch screen.
- **Show Broadcast Message on Touch Screen:** Turn the toggle on to show broadcast messages on the touch screen (broadcast messages are automatically shown on the display device).
- **Emergency Message Timeout:** Enter the number of minutes an emergency broadcast message is displayed on the touch screen.

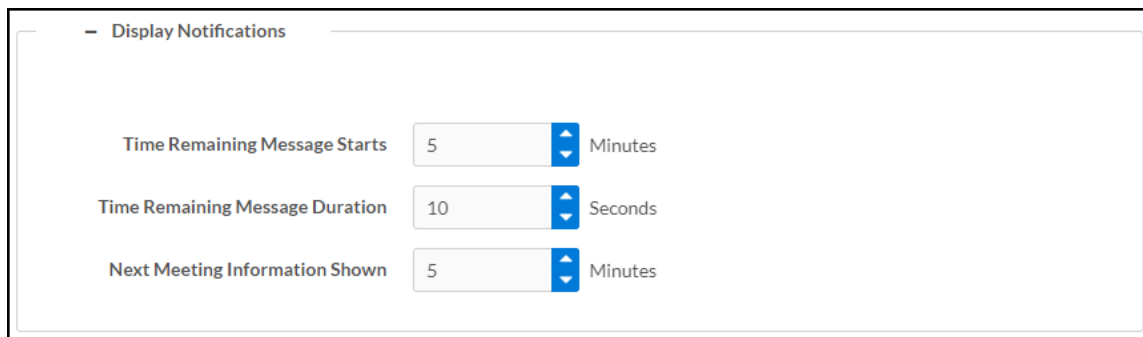
NOTE: Emergency broadcasts are sent from Crestron Fusion which is to be supported in a future firmware release. For more information on emergency broadcasts, refer to the [Crestron Fusion® Software SSI Model Reference Guide](#) (Doc. 7898).

- **Non-Emergency Message Timeout:** Enter the number of minutes a non-emergency broadcast message is displayed on the touch screen.

- **Touch Screen Auto Load:** Turn the toggle on to allow project files to be pushed to the touch screen from the cloud automatically.
- **.AV Framework User Interface Theme:** For future use.
- **Reservation:** Turn the toggle on to allow calendar reservations from the touch screen.
- **Touch Screen Custom Help:** Turn the toggle on to display a custom help screen when the information button is tapped on the touch screen. A **Custom Help URL** field appears. Enter the image's URL in the **Custom Help URL** field and save the changes.

Select the + (plus) icon next to **Display Notifications** to reveal settings for how notifications are displayed when an AirMedia device is in use.

Settings screen – Connected Devices (Display Notifications)



— Display Notifications

Time Remaining Message Starts 5 Minutes

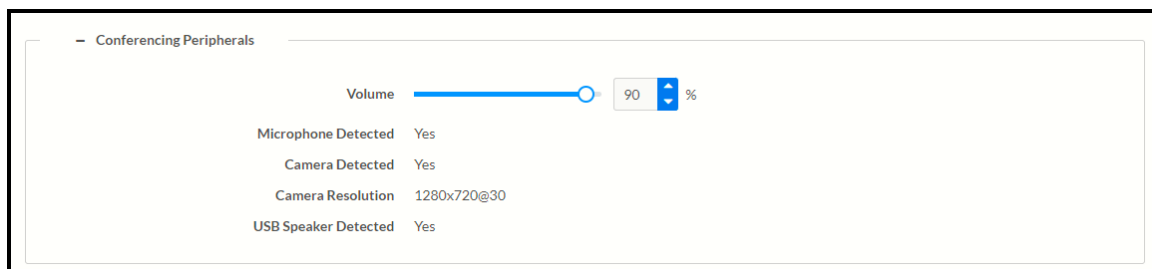
Time Remaining Message Duration 10 Seconds

Next Meeting Information Shown 5 Minutes

- **Time Remaining Message Starts:** Enter the amount of time that must pass (in minutes) before the meeting's time remaining message is displayed.
- **Time Remaining Message Duration:** Enter the amount of time (in seconds) that the time remaining message is displayed.
- **Next Meeting Information Shown:** Enter the amount of time (in minutes) before the next meeting's information is displayed.

Select the + (plus) icon next to **Conferencing Peripherals** to display settings and information for connected Wireless Conferencing peripherals.

Settings – Conferencing Peripherals



— Conferencing Peripherals

Volume 90 %

Microphone Detected Yes

Camera Detected Yes

Camera Resolution 1280x720@30

USB Speaker Detected Yes

- **Volume:** Controls the maximum allowed volume of connected USB speakers

NOTE: The volume slider will only appear when a supported peripheral device is connected.

- **Microphone Detected:** Indicates whether or not a microphone is connected
- **Camera Detected:** Indicates whether or not a camera is connected
- **Camera Resolution:** The resolution of a connected camera
- **USB Speaker Detected:** Indicates whether or not a USB speaker is connected

Routing

Select **Routing** to configure the order in which devices are routed to the display device upon connection.

Settings Screen – Routing

Routing

Input Routing

Routing Mode: Automatic Input Routing

Audio/Video Routes

Channel	Type	Display Name	Rank
	AirMedia	Wireless	1
	HDMI	HDMI	2

Select the + (plus) icons next to **Input Routing** and **Audio Video Routes** to display the **Routing Mode** setting and a list of the routed sources. By default, routing is automatic, meaning the last connected source will be routed to the display device.

Select one of the following routing modes from the dropdown list:

- **Automatic Input Routing:** Automatically route the last connected source to the display device.
- **Priority Routing:** Dictate the order in which sources are routed using the table in the **Audio/Video Routes** section.
 - To change the routing order of a device, select a number from the corresponding dropdown list under the **Rank** column. Devices with a lower number rank will take priority over others.
 - To change the name of the source that appears on the touch screen, type a name into the text field under the **Display Name** column in the corresponding row of the device.
- **AirMedia Auto-Route Only:** Automatically route a connected AirMedia source to the display device. Any other sources (HDMI, for example) must be manually routed from the touch screen.

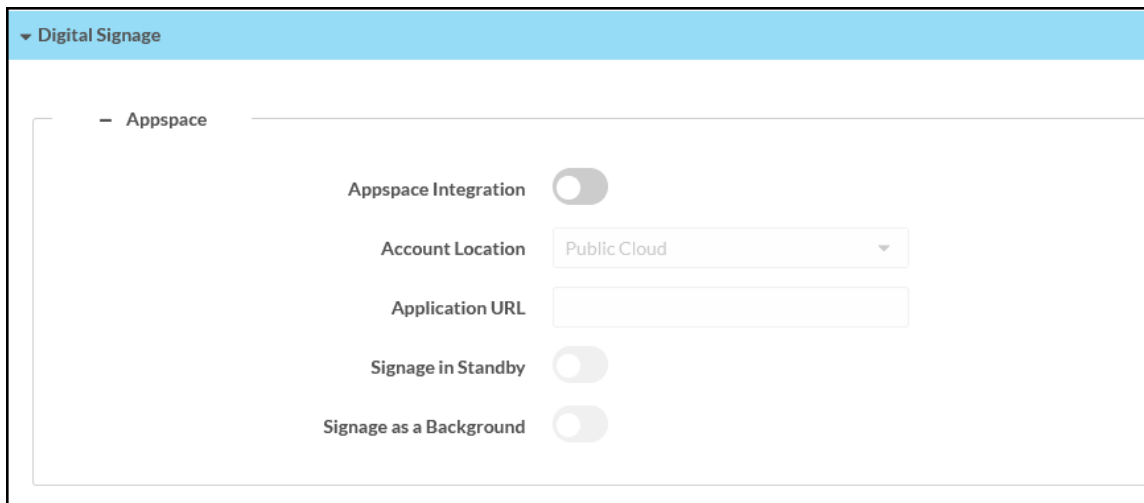
- **AirMedia Dock Upon Connect:** Automatically dock a source once it connects to the AirMedia receiver. When docked, the source does not present but remains connected to the display.

NOTE: The **AirMedia Dock Upon Connect** routing mode is available only for Windows or Android sources.

Digital Signage

Select **Digital Signage** to configure the device's operation with the Appspace platform. The AirMedia receiver can display content from an Appspace digital signage channel when no presentation is being made, or the room is not occupied.

Settings Screen – Digital Signage (Appspace)



NOTES:

- An active Appspace account is required.
- The Appspace video service is not supported.
- MicroSD card storage and touch screen support is not yet supported.
- Maximum resolution for all content should be 3840x2160 for optimal performance.
- **Appspace Integration:** Use the toggle button to enable the feature. The feature is used to integrate the Appspace digital signage application with AirMedia® Series 3 Receivers.

NOTE: To use Appspace, the receiver's Power Settings must be set to **Signage Only** as described in [Power Settings \(on page 29\)](#).
- **Account Location:** Select the location of the Appspace account from the drop-down list.
 - Select **Public Cloud** to use the Appspace public web app.
 - Select **Private Instance** to use a privately hosted instance of the Appspace web app

- **Application URL:** Enter the location of the privately hosted instance of the Appspace web app. Leave this field unfilled if **Public Cloud** is selected from the **Account Location** drop-down list.
- **Signage in Standby:** Turns on the display when the AirMedia receiver goes to sleep based on occupancy.
- **Signage as a Background:** Turns on the display along with the calendar, date/time, system name, connection info, and branding portions of the display.

NOTES:

- When the **Signage as a Background** toggle is turned on, the **Enable Custom Backgrounds** setting (described in [Connected Devices \(on page 47\)](#)) is disabled.
- For best practices on configuring the AirMedia receiver for use with Appspace, visit docs.appspace.com.

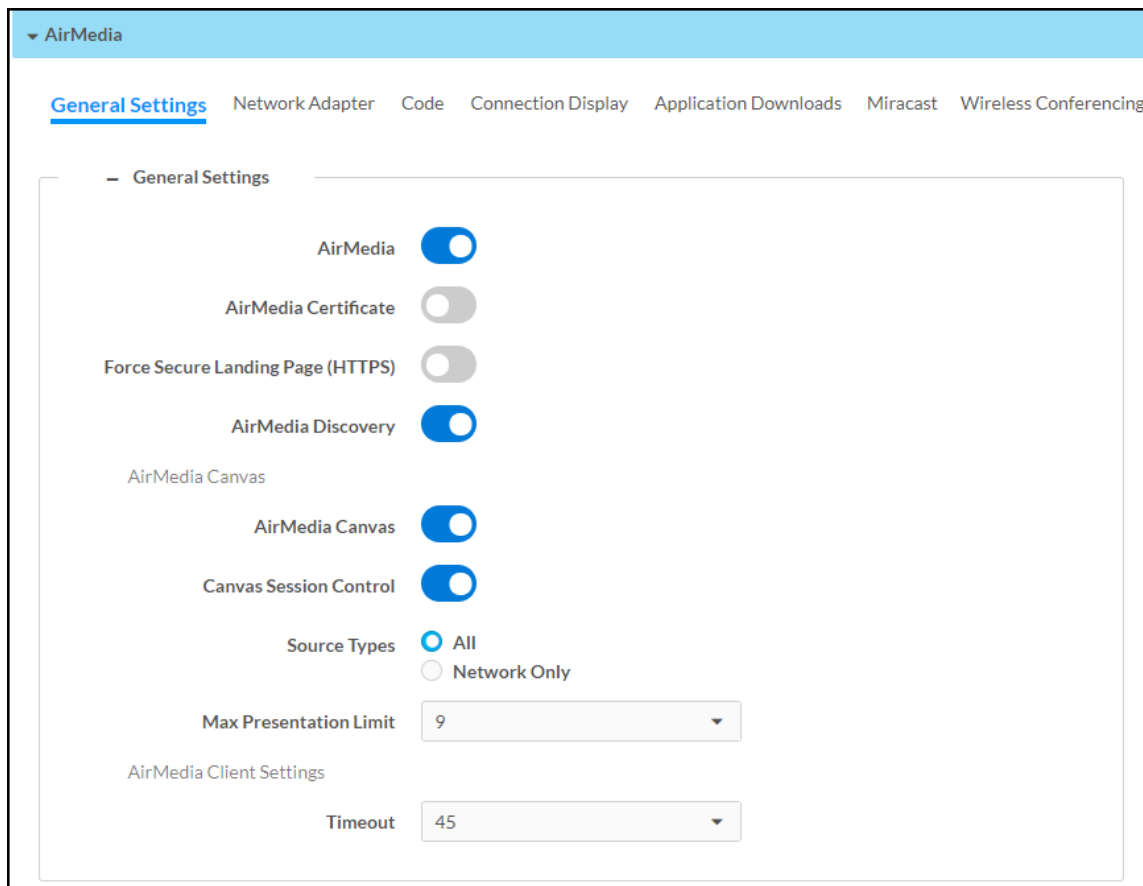
AirMedia

Select **AirMedia** to configure the device's AirMedia functionality.

AirMedia can support up to 30 simultaneously connected AirMedia application users (Windows or Android operating systems) and a maximum of two native mirroring users (Airplay or Miracast® mirroring). Up to four sources can present to the display simultaneously using the AirMedia Canvas feature. For details on the AirMedia canvas feature, refer to [AirMedia Canvas Functionality \(on page 58\)](#).

NOTE: For additional details on deploying AirMedia, refer to the [AirMedia Presentation Gateway Deployment Guide](#) (Doc 7693).

AirMedia Screen - General Settings



General Settings

Select the **General Settings** tab to configure settings for AirMedia, the AirMedia Canvas, and Miracast.

- **AirMedia:** Turn the toggle on to enable AirMedia wireless presentation on the AirMedia receiver.
- **AirMedia Certificate:** Turn the toggle on to use a third party certificate to encrypt connections between the sender applications for Windows and Android and the receiver. Load a certificate onto the device as described in [802.1x Configuration \(on page 72\)](#).
- **Force Secure Landing Page (HTTPS):** Turn the toggle on to force connecting devices to a secure landing page (HTTPS). When enabled, the web server uses either the certificate loaded in the certificate store (when available) or a self-signed certificate. The AirMedia connection URL will contain HTTPS.
- **AirMedia Discovery:** Turn the toggle on to allow the receiver to be automatically discovered by the AirMedia application on users' personal devices. When the toggle is turned off, users who wish to use present via AirMedia will be required to manually enter the receiver's IP address or host name.

- **AirMedia Canvas:** AirMedia Canvas allows multiple sources to present simultaneously on the display. Refer to [AirMedia Canvas Functionality \(on the facing page\)](#) for more information.
 - **AirMedia Canvas:** Turn the toggle on to enable AirMedia Canvas functionality.
 - **Canvas Session Control:** Turn the toggle on to control the AirMedia Canvas with a paired touch panel using the .AV Framework 2.0 Interface, a computer running the AirMedia client, or an iOS device running the AirMedia app.

NOTES: If **AirMedia Canvas** is disabled, **Canvas Session Control** can remain enabled. In this scenario, session controls are available for all connected users, but only one source can present at a time.

- **Source Types:** Select one of the radio buttons to select which sources can share space on the display. Select **All** to allow all source types (HDMI, AirMedia, Miracast, and AirPlay) to share space on the display. Select **Network Only** to allow only wireless sources (AirMedia, Miracast, and AirPlay) to share space on the display. HDMI sources will present in full screen if selected.
 - **Max Presentation Limit:** Select the maximum amount of sources that can present simultaneously.
- **AirMedia Client Settings**
 - **Timeout:** Select an amount of time (in minutes) before an inactive, connected user is automatically disconnected from the receiver. An inactive user is not actively presenting but still connected to the receiver.

AirMedia Canvas Functionality

AirMedia Canvas allows multiple sources to present simultaneously on the display. AirMedia Canvas automatically configures the best possible layout to maximize screen coverage based on the number of active sources, the type of sources, their orientation, and their aspect ratios.

The following sources can share space on a display simultaneously:

- AirMedia (Windows, Android, Mac, iOS, AirPlay/Miracast)

NOTE: The AirMedia extension for Chrome OS is not supported and will only be allowed to present full screen.

- HDMI

NOTE: When the AirMedia Canvas feature is enabled, the 4:2:0 color space is used for high definition sources connected to the HDMI input port. When the AirMedia Canvas feature is disabled, the 4:4:4 color space is used. If the 4:4:4 color space is required by sources connected to the HDMI input port, the AirMedia Canvas should be disabled.

When enabled, AirMedia Canvas works as follows:

- If one source is active, the source presents in full screen.
- If multiple sources are active, the sources present in a way that maximizes screen coverage depending on their aspect ratios.
- When multiple sources are active, and all but one of the sources is disconnected, the single source returns to full screen.
- If the maximum amount of sources is reached and another source is selected, then the first active source is docked (AirMedia user) or disconnected (hard wired inputs, AirPlay connection, or Miracast connection). When docked, the source stops presenting but remains connected to the display.
- When all sources are disconnected, the display shows the front of the room experience splash screen.

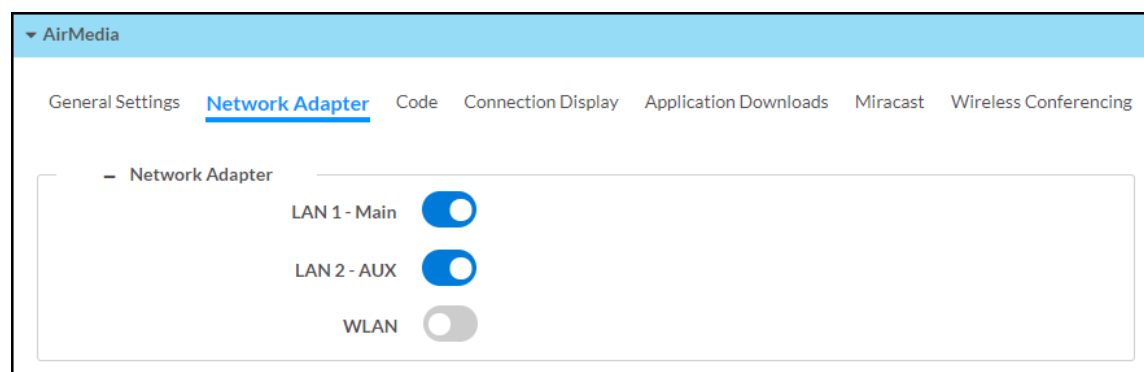
When AirMedia Canvas is disabled, the display shows one source at a time.

For details on using a touch screen to control AirMedia Canvas, refer to [AirMedia Canvas \(on page 112\)](#). For details on using a computer or iOS device to control AirMedia canvas, refer to [Share Content \(on page 91\)](#).

Network Adapter

Select the **Network Adapter** tab to determine the Ethernet ports assigned for use by AirMedia.

AirMedia Screen - Network Adapter



- **LAN 1 - Main:** Turn the toggle on to allow AirMedia connections from the local area network.
- **LAN 2 - AUX:** (AM-3200(-WF)(-I) models only) Turn the toggle on to allow AirMedia connections from a secondary, guest-only local area network. For more information on the second LAN connection, refer to [Dual LAN Functionality \(AM-3200\(-WF\)\(-I\) models only\) \(below\)](#).
- **WLAN:** Allow AirMedia connections from the receiver's self hosted Wi-Fi access point (Wi-Fi network enabled models only).

Dual LAN Functionality (AM-3200(-WF)(-I) models only)

AirMedia Series 3 receivers provide dual LAN connectivity for isolated internal and guest networks. Users may present via AirMedia or connect to the receiver's web configuration interface when connected to either network.

The secondary LAN port is intended solely for use with a guest network. The secondary LAN port has limited functionality and does not support the following devices and services:

- XiO Cloud service
- Crestron Fusion software
- Scheduling services (such as Google Calendar or Microsoft 365 software)
- Occupancy sensors
- Touch screen control
- ChromeOS presentation
- Power over Ethernet

Make LAN connections to the receiver as described in the [AM-3200, AM-3200-WF, and AM-3200-WF-I Quick Start guide](#) (Doc. 8986).

Code

Select the **Code** tab to configure the access code that must be entered to present content on the AirMedia receiver.

AirMedia Screen - Code

▼ AirMedia

General Settings Network Adapter **Code** Connection Display Application Downloads Miracast Wireless Conferencing

— Code

Show Login Code ☒

Login Code Mode ☐ Disabled ☒ Random ☐ Fixed

Login Code

- **Show Login Code:** Turn the toggle on to show the access code on the display device.
- **Login Code Mode:** Select a radio button to specify how the access code is used.
 - **Disabled:** Allows any user with the device's IP address or host name to open a client connection without entering an access code.
 - **Random:** Randomly generates an access code. A new code is generated when the last connected presenter disconnects from the device. The access code is shown on the display device when AirMedia is selected.
 - **Fixed:** Uses a user-specified, four-digit access code. Enter a custom code in the **Login Code** field when **Fixed** is selected.

Connection Display

Select the **Connection Display** tab to configure how AirMedia connection details are shown on a connected display device.

NOTE: For more details on how AirMedia connection details are shown on a display device, refer to [Front of Room Experience \(on page 87\)](#).

AirMedia Screen - Connection Display

▼ AirMedia

General Settings Network Adapter Code Connection Display Application Downloads Miracast Wireless Conferencing

— Connection Display

LAN Connection Information

Show AirMedia Connection Info Overlay ☒

Show Airplay Info ☒

Show Connection Info ☒

Connection URL Mode ☒ IP Address ☐ Host ☐ Host and Domain ☐ Custom

Custom URL *

Additional Connection Information

Show Connection Info ☒

Info Mode

Connection Info Mode ☒ IP Address ☐ Host ☐ Host and Domain ☐ Custom

Custom URL *

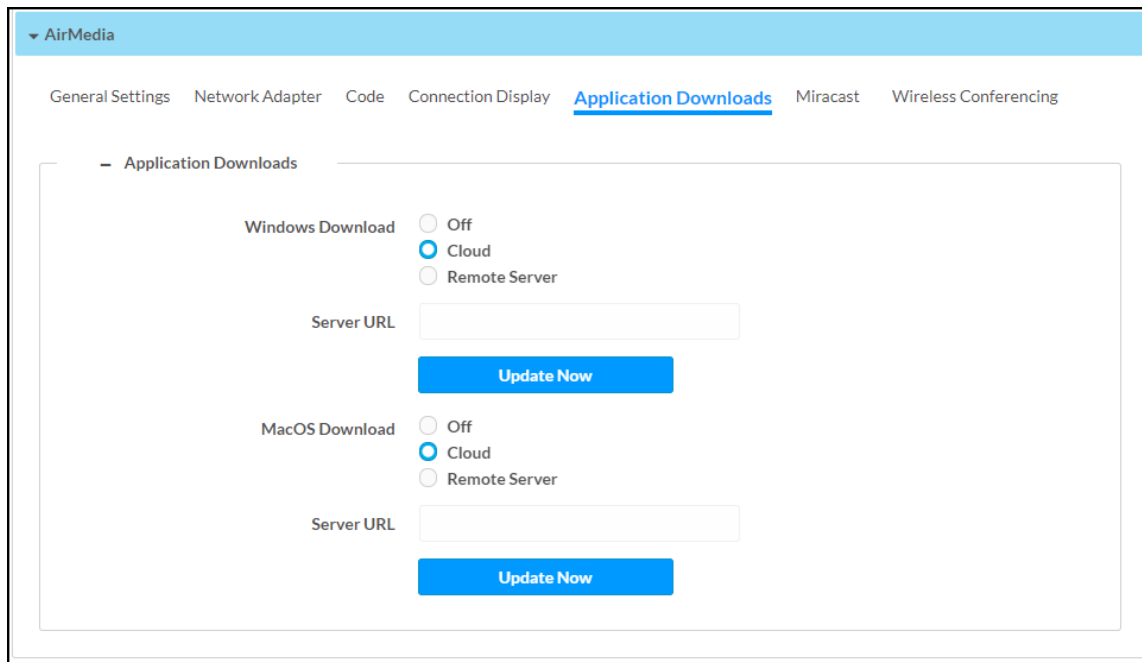
- **Show AirMedia Connection Info Overlay:** Turn the toggle on to show connection information on the display device when a user is presenting. Crestron recommends turning this setting on.
- **Show Airplay Info:** Turn the toggle on to show Airplay connection information on the display.
- **LAN Connection Information**
 - **Show Connection Info:** Turn the toggle on to display connection information on the display device.
 - **Connection URL Mode:** Select one of the radio buttons to decide what connection information is shown on the display device.
 - **IP Address:** Show the IP address used to connect to the receiver.
 - **Host:** Show the host name used to connect to the receiver.
 - **Host and Domain:** Show the host name and domain name used to connect to the receiver.
 - **Custom:** Show a custom URL used to connect to the receiver. Enter the custom URL in the **Custom URL** field.

- **WLAN Connection Information:** The receiver can be configured to show Wi-Fi connection information on the display device.
 - **Show Connection Info:** Turn the toggle on to show Wi-Fi connection information on the display device.
 - **WiFi Info Mode:** Select what Wi-Fi network information to show from the dropdown menu.
 - Select **Internal WiFi Access Point** to show the internal access point's connection information on the display device.
 - Select **Specify WiFi Internal Info** to define and show SSID and connection key information on the display device. Turn on the respective toggles to show SSID and connection key information, and enter the SSID and connection key information into the respective fields.
 - **Connection Info Mode:** Select one of the radio buttons to decide what connection information is shown on the display device.
 - **IP Address:** Show the IP address used to connect to the receiver.
 - **Host:** Show the host name used to connect to the receiver.
 - **Host and Domain:** Show the host name and domain name used to connect to the receiver.
 - **Custom:** Show a custom URL used to connect to the receiver. Enter the custom URL in the **Custom URL** field.

Application Downloads

Select **Application Downloads** to configure how AirMedia client applications are presented to the user for download. Client applications are required to present from a user's computer as described in [Present with AirMedia \(on page 89\)](#).

AirMedia Screen - Application Downloads



The screenshot shows the 'AirMedia' settings interface. At the top, there's a blue header with 'AirMedia' and a dropdown arrow. Below it, a navigation bar contains links: 'General Settings', 'Network Adapter', 'Code', 'Connection Display', 'Application Downloads' (which is underlined and highlighted), 'Miracast', and 'Wireless Conferencing'. The main content area is titled 'Application Downloads' and contains two sections. The first section is for 'Windows Download' with three radio buttons: 'Off', 'Cloud' (which is selected), and 'Remote Server'. Below these is a 'Server URL' text input field and a blue 'Update Now' button. The second section is for 'MacOS Download' with three radio buttons: 'Off', 'Cloud' (which is selected), and 'Remote Server'. Below these is another 'Server URL' text input field and a blue 'Update Now' button.

Select a radio button for the **Windows Download** and **MacOS Download** settings to decide how AirMedia client applications are presented to users according to their computer's operating system:

- **Off:** Provide the version of the AirMedia application included with the receiver's firmware.
- **Cloud:** Provide the latest version of the AirMedia application stored in the Cloud. The receiver checks for an update once a day at 2:00 am (local time).
- **Remote Server:** Provide a version of the AirMedia application that is hosted on a remote server. When selected, enter the URL of the remote server in the **Server URL** field.
- **Update Now:** Update the AirMedia application according to the **Windows Download** or **MacOS Download** setting.

NOTE: If the setting is changed from **Cloud** or **Remote Server** to **Off**, the receiver will provide the application version that is included with the device's firmware (even if it is an older version than what is available in the cloud or the remote server).

Miracast

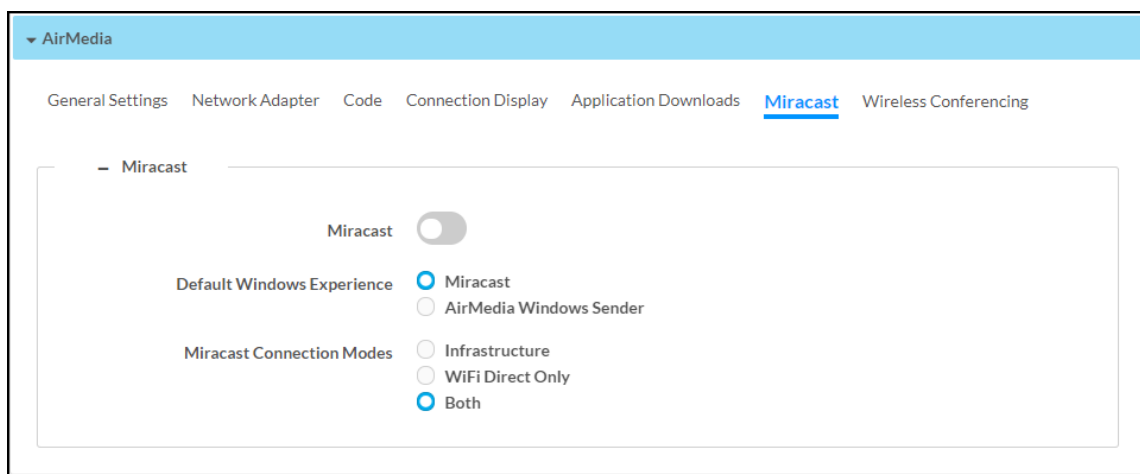
Miracast technology allows users to wirelessly share content from a Microsoft® Windows® 10 device to the receiver. Miracast technology is built into the Microsoft Windows 10 operating system, so no additional software installation is required.

NOTE: Refer to the [AirMedia Presentation Gateway Security Reference Guide](#) (Doc 7693) for best practices for configuring the system for Miracast.

A Miracast connection consists of two phases: the discovery phase and the connection phase. During the discovery phase, the Windows 10 device uses Wi-Fi based discovery to find compatible receivers. Once the receiver is discovered by the Windows 10 device, it is presented in a list on the device. The user can then select the receiver for connection to the Windows 10 device.

During the connection phase, the Windows 10 device will first attempt to connect to the receiver through the existing network infrastructure. If the connection over infrastructure fails, the Windows 10 device will connect to the receiver.

AirMedia Screen - Miracast



- **Miracast:** Turn the toggle on to enable Miracast on the receiver.
- **Default Windows Experience:** Select one of the radio buttons (**Miracast** or **AirMedia Windows Sender**) to select the default connection experience for Windows 10 users when they connect to the receiver via a web browser.
 - Select **Miracast** to display instructions for connecting to the receiver via Miracast.
 - Select **AirMedia Windows Sender** to prompt the user to download the AirMedia sender application.

- **Miracast Connection Modes:** Select one of the radio buttons (**Infrastructure**, **WiFi Direct Only**, or **Both**) to configure how a Miracast capable device connects to the receiver.
 - Select **Infrastructure** to connect via the local area network. When selected, Wi-Fi is used for discovery only.
 - Select **WiFi Direct Only** to connect via a Wi-Fi point-to-point connection (Wi-Fi Direct® connection). When selected, Wi-Fi is used for discovery and for streaming.
 - Select **Both** to connect via a local area network or Wi-Fi point-to-point connection (Wi-Fi Direct® connection). When selected, a Wi-Fi point-to-point connection only occurs if the local area connection fails.

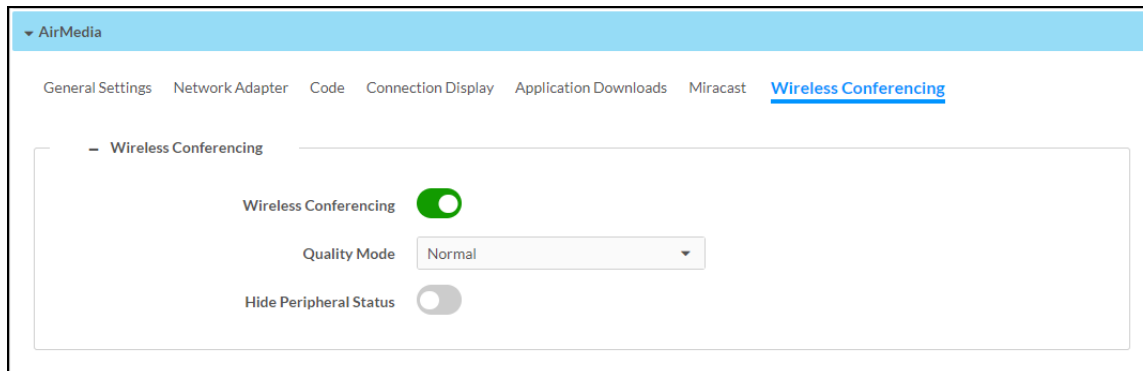
NOTE: When **WiFi Direct Only** or **Both** is selected, **Login Code Mode** must be set to **Random** or **Fixed** as described in [Code \(on page 59\)](#).

Wireless Conferencing

Select **Wireless Conferencing** to configure settings for the Wireless Conferencing feature. Wireless Conferencing allows the receiver to use connected conferencing peripherals, such as soundbars, cameras, or speakerphones when the user makes a call from a meeting room application.

For a list of peripherals supported with Wireless Conferencing, refer to [Online Help 1001764](#).

AirMedia Screen - Wireless Conferencing



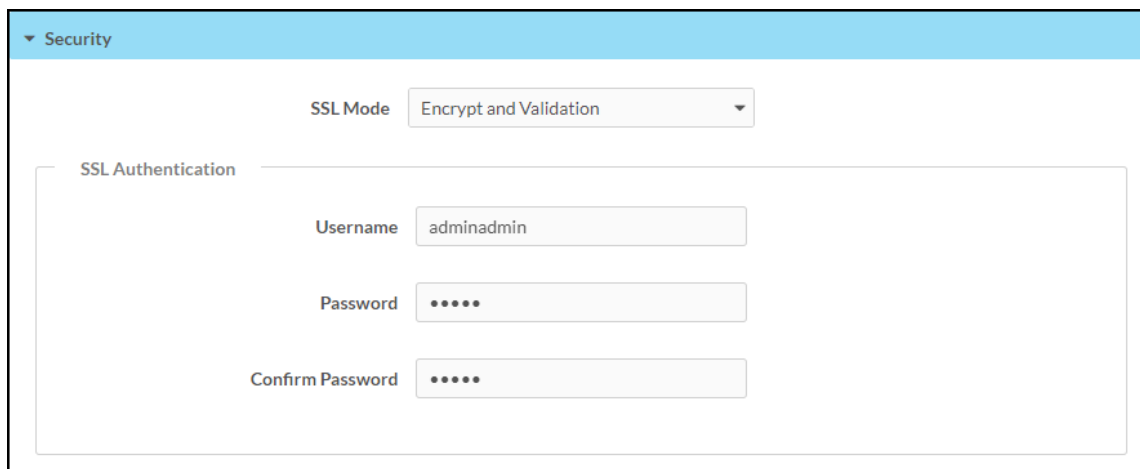
- **Wireless Conferencing:** Turn the toggle on to enable Wireless Conferencing on the receiver. PoE+ or a local power supply is required to enable Wireless Conferencing.
- **Quality Mode:** Select the video quality of a connected camera from the dropdown menu.
 - Select **Normal** to display the standard video quality of the camera.
 - Select **Low** to display a lowered level of video quality. **Low** should only be selected if there are network bandwidth concerns that arise when **Normal** is selected.
- **Hide Peripheral Status:** Turn the toggle on to hide the peripheral status from the display when Wireless Conferencing is in use.

For more information on Wireless Conferencing, refer to the [AirMedia Presentation Gateway Security Reference Guide](#) (Doc 7693).

Security

Select **Security** to configure device security and authentication settings.

Security – Authentication Management



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

Authentication

By default, authentication is required to access the web configuration interface or to connect to an AirMedia Series 3 receiver through Crestron Toolbox™ software. When a user attempts to sign into the device for the first time, the web configuration interface prompts the user to enter a new administrator username and password as described in [Connect to the Receiver \(on page 5\)](#). This username and password will be saved and must be entered when reconnecting to the receiver in the future.

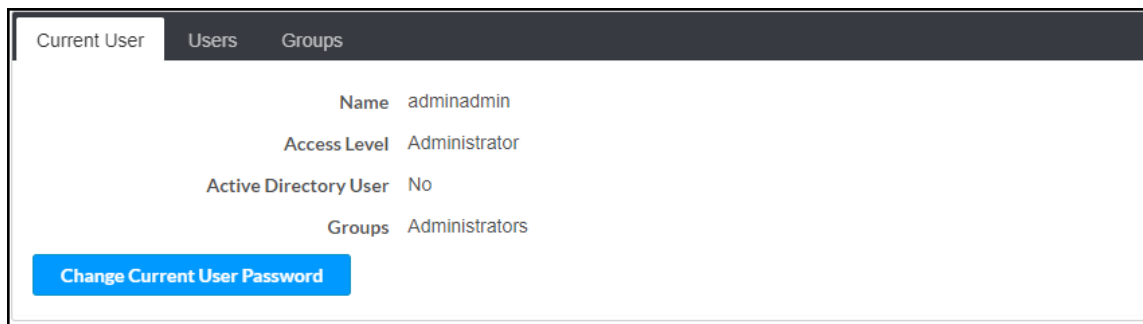
CAUTION: Do not lose the administrator username and password, as the receiver settings must be restored to factory defaults to reset the username and password. To restore the device to factory defaults, refer to [Restore \(on page 9\)](#).

Use the following **Authentication Management** settings to add, delete, and edit users and groups.

Current User

Select **Current User** to view and edit information for the current receiver user.

Authentication Management - Current User



Name	adminadmin
Access Level	Administrator
Active Directory User	No
Groups	Administrators

[Change Current User Password](#)

The following settings are displayed for the current user:

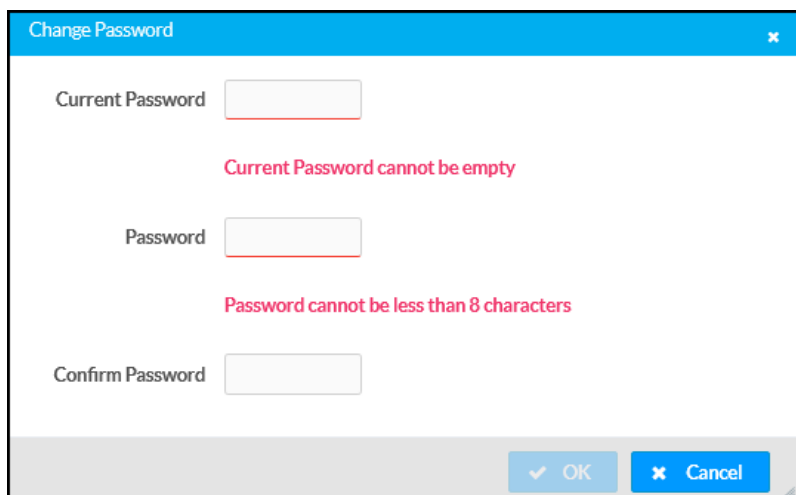
- **Name:** The chosen username
- **Access Level:** The access level granted to the user (**Administrator**, **Connect**, **Operator**, **Programmer**, or **User**)
- **Active Directory User:** Reports whether the current user is (**Yes**) or is not (**No**) authenticated through Active Directory® software

NOTE: A user must be added to an Active Directory group before the user may be selected as an active directory user. For more information, refer to [Groups \(on page 69\)](#).

- **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



Change Password

Current Password

Current Password cannot be empty

Password

Password cannot be less than 8 characters

Confirm Password

OK Cancel

Enter the existing password in the **Current Password** field. Then, enter a new password in the **Password** field, and reenter the password in the **Confirm Password** field.

Select **OK** to save the new password, or select **Cancel** to cancel the change.

Users

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

Authentication Management - Users

Username	AD User	Action
adminadmin	No	  

Create User

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

Receiver users are listed in table format. The following information is displayed for each 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 \(on the next page\)](#).

If the receiver 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.

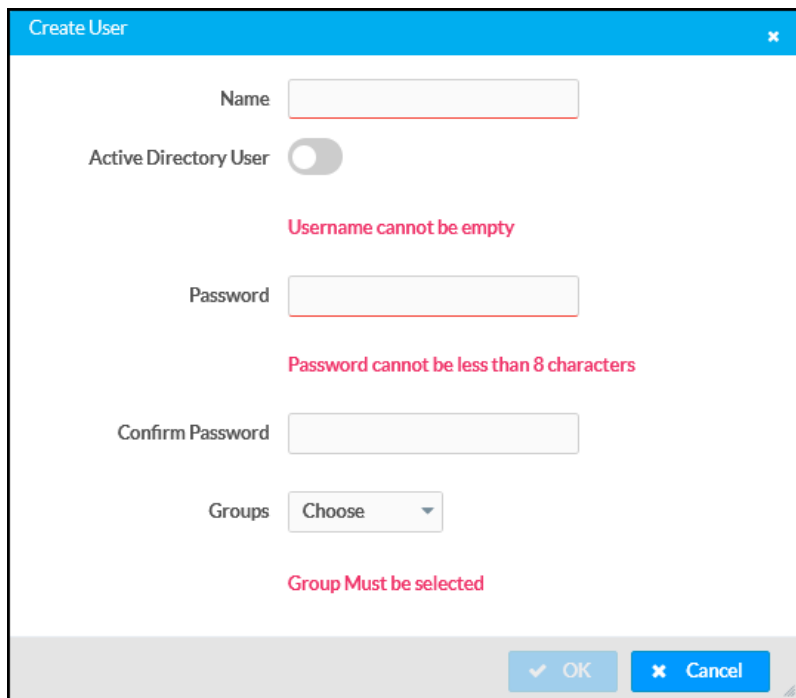
An **Action** column is also provided for each user that allows various actions to be performed. The following selections may be selected from the **Action** column:

- Select the information button  to view a user's username, Active Directory status, and group membership.
- Select the edit button  to edit a user's password and group membership.
- Select the trashcan button  to delete a user.

Create User

Select **Create User** to create a new user. The **Create User** dialog box is displayed.

Create User Dialog Box

The image shows a 'Create User' dialog box with a blue title bar. It contains several input fields and a toggle switch. The 'Name' field is empty, with a red error message 'Username cannot be empty' below it. The 'Active Directory User' toggle is turned off. The 'Password' field is empty, with a red error message 'Password cannot be less than 8 characters' below it. The 'Confirm Password' field is empty. The 'Groups' dropdown menu is set to 'Choose', with a red error message 'Group Must be selected' below it. At the bottom right, there are 'OK' and 'Cancel' buttons.

- **Name:** The chosen username
- **Active Directory User:** Turn on the toggle to use authentication via Active Directory for the selected user.
- **Password:** Enter a new password for the selected user.
- **Confirm Password:** Reenter the password provided in the **Password** field.
- **Groups:** Add the user to one or more groups. For more information, refer to [Groups \(below\)](#).

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 **Authentication Management > Users** page. Select **Cancel** to cancel any changes.

Groups

Select **Groups** to view and edit settings for receiver groups. Receiver groups are used to group users by access level and Active Directory authentication settings.

Authentication Management - Groups

Current User Users Groups			
Search...			
Group Name	AD Group	Access Level	Action
Administrators	No	Administrator	 
Connects	No	Connect	 
Operators	No	Operator	 
Programmers	No	Programmer	 
Users	No	User	 
1 10			
Create Group			

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

Groups are listed in table format. The following information is displayed for each group:

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

If the receiver 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.

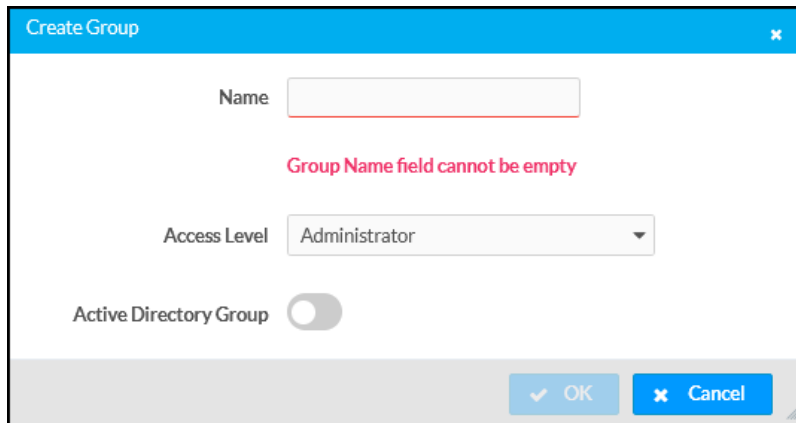
An **Action** column is also provided for each group that allows various actions to be performed. The following selections may be selected from the **Action** column:

- Select the information button  to view a group's name, access level, and Active Directory status.
- Select the trashcan button  to delete a user.

Create Group

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

Create Group Dialog Box

A screenshot of the 'Create Group' dialog box. The dialog has a blue title bar with the text 'Create Group' and a close button. Inside, there is a 'Name' label followed by an empty text input field. Below the input field is a red error message: 'Group Name field cannot be empty'. Underneath is an 'Access Level' label followed by a dropdown menu showing 'Administrator'. At the bottom left is an 'Active Directory Group' label with a toggle switch that is currently turned off. At the bottom right are two buttons: 'OK' with a checkmark icon and 'Cancel' with an 'x' icon.

The following **Create Group** settings may be viewed or configured:

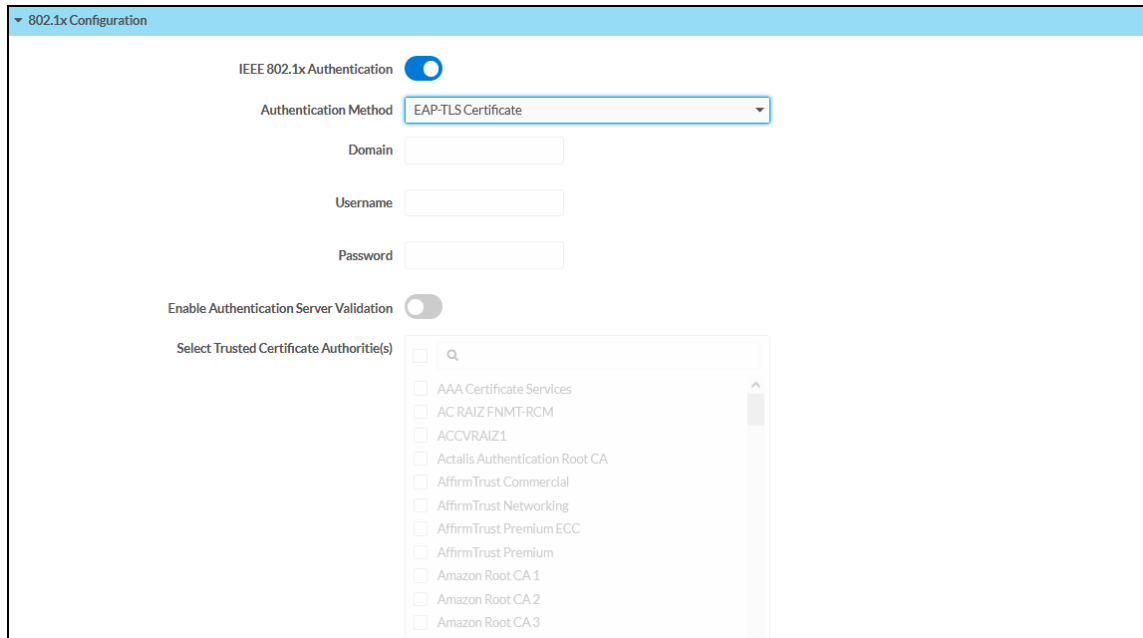
- **Name:** Enter a group name
- **Access Level:** Select an access level for the group and its users from the dropdown menu
- **Active Directory Group:** Turn on the toggle to use authentication via Active directory for the group

Select **OK** to save any changes and to return to the **Authentication Management > Groups** page.
Select **Cancel** to cancel any changes.

802.1x Configuration

Select **802.1x Configuration** to display selections for configuring IEEE 802.1x network authentication for receiver security.

802.1x Configuration Tab Selections

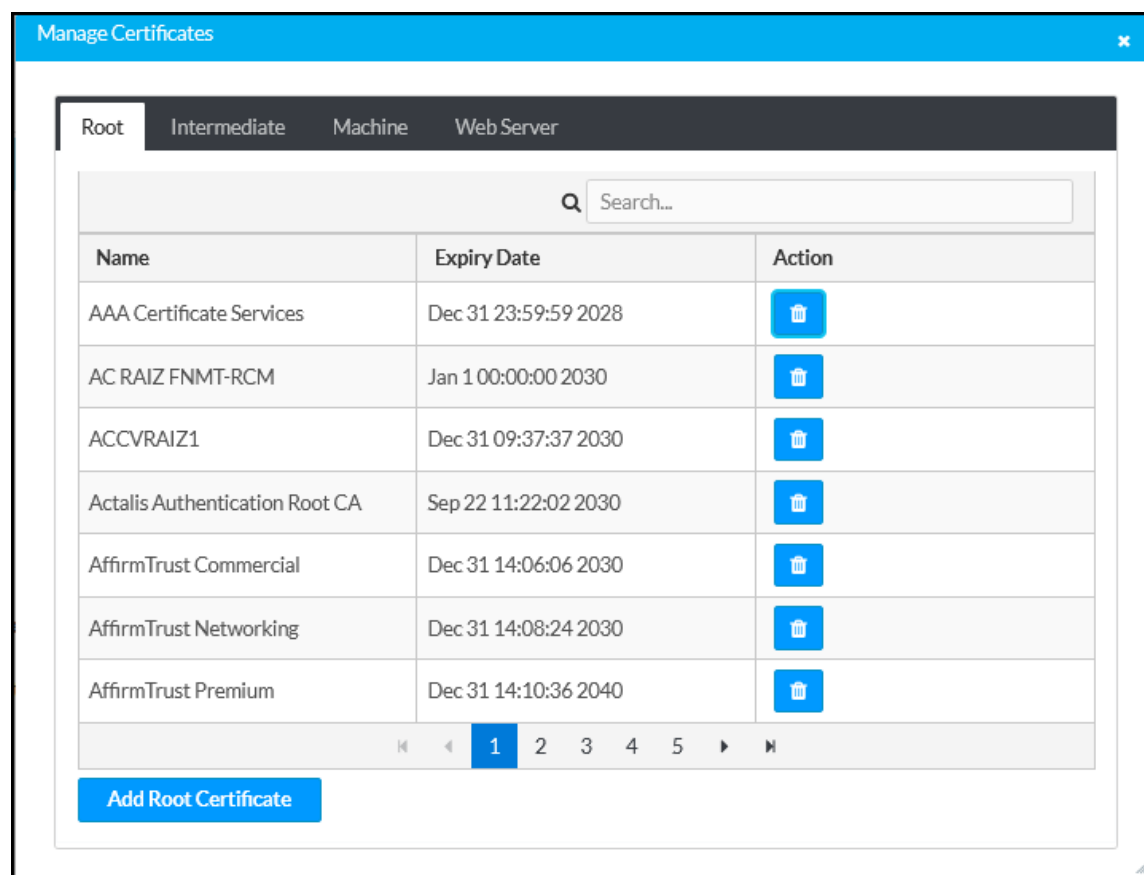


The screenshot shows the '802.1x Configuration' tab. At the top, there is a toggle for 'IEEE 802.1x Authentication' which is turned on. Below this is a dropdown menu for 'Authentication Method' currently set to 'EAP-TLS Certificate'. Underneath are three input fields for 'Domain', 'Username', and 'Password'. Further down is another toggle for 'Enable Authentication Server Validation' which is turned off. At the bottom, there is a section titled 'Select Trusted Certificate Authoritie(s)' with a search bar and a list of certificate authorities. The list includes: AAA Certificate Services, AC RAIZ FNMT-RCM, ACCVRAIZ1, Actalis Authentication Root CA, AffirmTrust Commercial, AffirmTrust Networking, AffirmTrust Premium ECC, AffirmTrust Premium, Amazon Root CA 1, Amazon Root CA 2, and Amazon Root CA 3. Each item has a checkbox to its left.

- **IEEE 802.1x Authentication:** Turn on the toggle to use 802.1x authentication for the receiver.
- **Authentication Method:** Select an 802.1x authentication method (**EAP-TLS Certificate** or **EAP MSCHAP V2- password**) from the dropdown menu.
- **Domain:** If **EAP MSCHAP V2- password** is selected for **Authentication Method**, enter a domain name for authentication.
- **Username:** If **EAP MSCHAP V2- password** is selected for **Authentication Method**, enter a username for authentication.
- **Password:** If **EAP MSCHAP V2- password** is selected for **Authentication Method**, enter a password for authentication.
- **Enable Authentication Server Validation:** Turn on the toggle to use server validation for elevated security.
- **Select Trusted Certificate Authorities:** Select trusted CAs (Certificate Authorities) from the provided CAs to be used for server validation:
 - Select the corresponding check box for each CA that you wish to make a trusted CA.
 - Enter a search term into the text field to search for and display CAs that match the search term.
 - Select the check box in the search field 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.

Manage Certificates Dialog Box - Root Tab



Select **Root**, **Intermediate**, **Machine**, or **Web Server** to switch between the different types of CAs. The same settings are provided for each type of CA.

Enter 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:

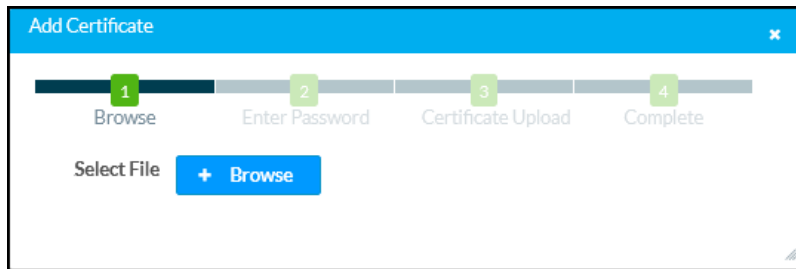
- **Name:** The CA name
- **Expiry Date:** The date and time that the CA is set to expire

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.

Select the trashcan button in the **Action** column for a CA to delete it. Select **Yes** to delete the certificate or **No** to cancel.

Select **Add [Type] Certificate** to add a 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.

Add Certificate Dialog Box – Browse



To add a new certificate:

1. Select **Browse**.
2. Navigate to the CA file on the host computer.
3. Select the CA file, and then select **Open**.
4. If required, enter the password used to encrypt the file.
5. Select **Load** to load the CA file to the receiver. The upload progress is shown in the dialog box.
6. Once the receiver has completed the upload, select **OK**.

Select the **x** button to close the **Add Certificate** dialog box at any time during the upload process. Selecting the **x** button before the CA file is uploaded to the touch screen cancels the upload.

Select the **x** button to close the **Manage Certificates** dialog box and to return to the **802.1x Authentication** page.

Enterprise Deployment Options

Crestron has two options for deploying multiple AirMedia receivers across an enterprise. These tools can assist in deploying any number of receivers that an organization may need to deploy.

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 www.crestron.com/Support/Tools/Licensing-Registration/XiO-Cloud-Registration-Room-Licenses.

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 Deployment Tool for PowerShell® Software

Crestron has developed a tool for customers without the ability to use CPS to assist in deploying multiple devices without the need to configure each device individually. With this tool, an administrator has the ability to input all of the settings to be configured on multiple receivers, and then use PowerShell® task-based command-line shell and scripting language to configure the devices across a local network.

Modern Authentication for EWS

This appendix provides the procedures required to configure Modern Authentication (OAuth 2) support for AirMedia series 3 receivers in the Microsoft® EWS (Exchange Web Services) service.

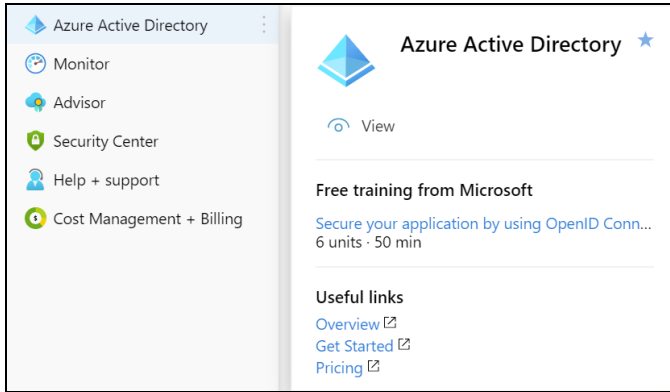
The Modern Authentication authorization model is provided by the Azure® Active Directory® service to integrate managed API applications with the same authentication model used by the Microsoft 365 software REST APIs. Once Modern Authentication is configured in EWS, the AirMedia receiver uses this access method to provide heightened user authentication.

Use the following procedures to define a new application in Azure Active Directory. Once the application is defined, multiple Crestron devices can leverage calendar integration with Microsoft 365 and Modern Authentication without additional setup in the Microsoft EWS service.

Create the Application

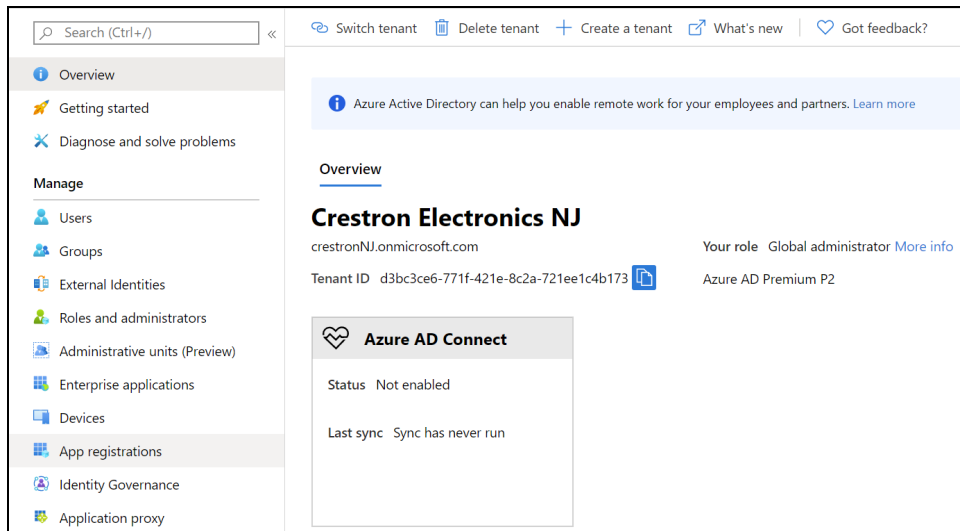
1. Sign into the Azure portal with a user ID with sufficient permissions to create an app.
2. Select **Azure Active Directory** from the navigation menu.

Azure Active Directory Selection



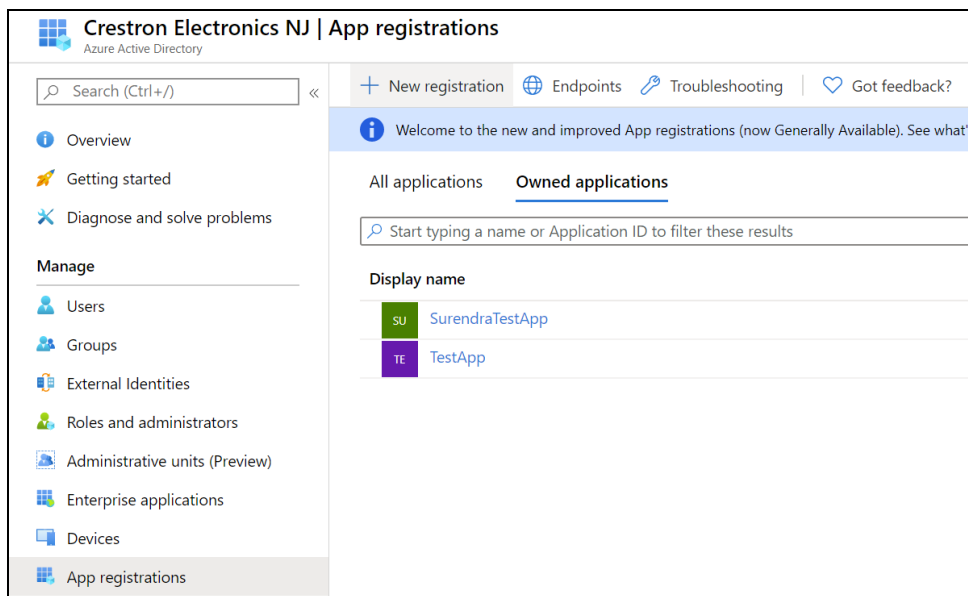
3. Select **App registrations** from the Azure widget menu.

App registrations Selection



4. Select **+ New registration**.

App registrations - New registration Screen



A dialog box for creating the app is displayed.

Register an application Dialog Box

Home > Crestron Electronics NJ | App registrations > Register an application

Register an application

*** Name**
The user-facing display name for this application (this can be changed later).
Crestron Scheduling Device ✓

Supported account types
Who can use this application or access this API?

☒ Accounts in this organizational directory only (Crestron Electronics NJ only - Single tenant)
☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web ▼ e.g. https://myapp.com/auth

5. Enter the following information:

- **Name:** Enter a user-facing name of the application (in the Azure environment). This can be any string 120 characters or less. It is possible to have more than one application registered with the same display name.
- **Supported account types:** Select the supported account type. Only the **Accounts in this organizational directory only** option is supported by the AirMedia receiver at this time.

NOTE: The **Redirect URI (optional)** settings are not configured for this application.

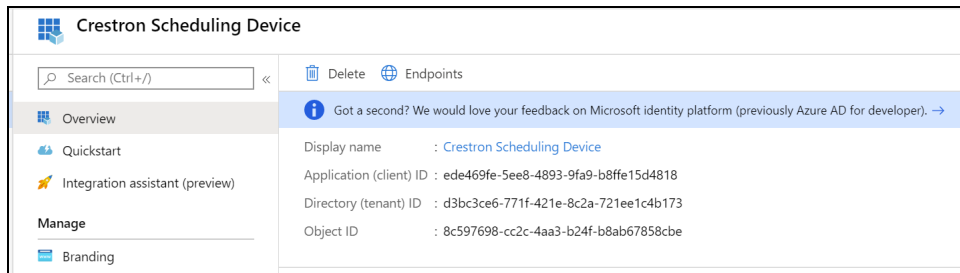
6. Select **Register**.

Obtain Authentication IDs

Once the app is registered, the application and directory IDs must be obtained to connect the receiver to the Azure AD app.

1. Select **App registrations** from the Azure widget menu.
2. Select the application created for the receiver. An application dialog box is displayed.
3. Select **Overview** from the navigation menu. Information about the Azure app is provided.

Application Overview Screen



4. Copy the following fields from the **Overview** pane to an accessible location. Use the **Copy to Clipboard** button that appears when hovering over each field to ensure accuracy.
 - **Application (client) ID:** The unique identification string for the Azure app.
 - **Directory (tenant) ID:** The unique identification string for the Azure directory.

Configure Additional Settings

The following additional settings can be configured for the Azure app. These settings define the user consent experience, authentication details, and API access scopes available to the application.

Branding

Select **Branding** under the **Manage** section of the application navigation menu to configure branding settings for the app.

Application Branding Screen

Home > Crestron Electronics NJ | App registrations > Crestron Scheduling Device | Branding

Crestron Scheduling Device | Branding

Search (Ctrl+/) Save Discard

Overview

Quickstart

Integration assistant (preview)

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

Owners

Roles and administrators (Previ...

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Name * Crestron Scheduling Device

Logo

Upload new logo

Home page URL

Terms of service URL

Privacy statement URL

Publisher domain crestronNJ.onmicrosoft.com [Update domain](#)

The application's consent screen will show 'Unverified'.
[Learn more about publisher domain](#)

Publisher verification (preview)

Associate a verified Microsoft Partner Center (MPN) account with your application. A verified badge will appear in various places, including the application consent screen. [Learn more](#)

MPN ID

[Add MPN ID to verify publisher](#)

The application publisher domain is set to crestronNJ.onmicrosoft.com, but onmicrosoft.com publisher domains are not allowed. Please use a custom domain in order to proceed. Note: this domain must be a DNS verified domain on the tenant and match the primary contact domain for your MPN account.

Publisher display name Not provided

The following branding settings can be configured for the application:

- **Name: Required.** Set the user-friendly name of the application. This is the same name that was defined when registering the application, but it can be changed here.
- **Upload New Logo:** Set a user-facing logo for this application that appears on the consent screen. The image file for the logo must meet the following requirements:
 - Image dimensions of 215 x 215 pixels
 - Central image dimensions of 94 x 94 pixels
 - Uses the file type .bmp, .jpg, or .png
 - File size less than 100 KB
- **Privacy statement URL:** Provides a link to the application privacy statement in the consent screen.
- **Publisher domain:** Sets the process that must be completed to verify ownership of the domain. Most users will probably already have a verified domain. If the domain is not verified, the application will work, but the consent screen will warn the user they are consenting to an unverified application.

Authentication

Select **Authentication** under the **Manage** section of the application navigation menu to configure authentication settings for the app.

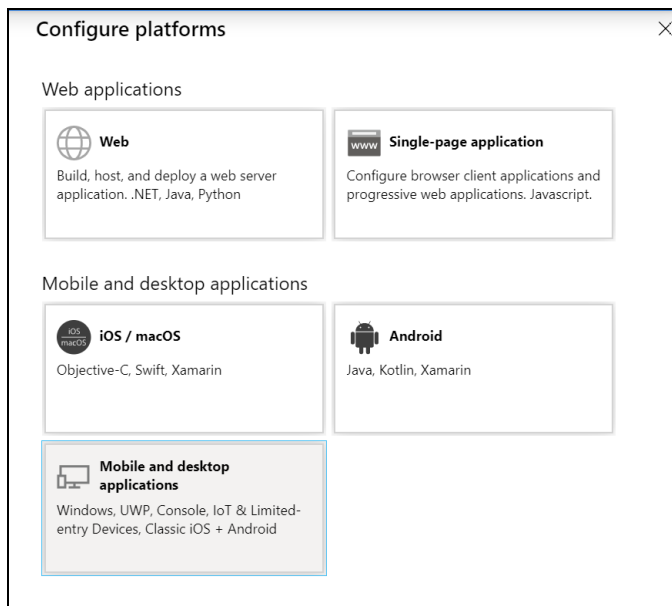
Application Authentication Screen

The screenshot shows the 'Authentication' configuration page for a 'Crestron Scheduling Device'. The page has a left-hand navigation menu with sections: Overview, Quickstart, Integration assistant (preview), Manage (selected), Certificates & secrets, Token configuration, API permissions, Expose an API, Owners, Roles and administrators (Preview), Manifest, Support + Troubleshooting, Troubleshooting, and New support request. The 'Manage' section is expanded, showing 'Authentication' as the active item. The main content area is titled 'Crestron Scheduling Device | Authentication' and includes a search bar, 'Save', 'Discard', and 'Got feedback?' buttons. The content is organized into three sections: 'Platform configurations' with an 'Add a platform' button; 'Supported account types' with radio buttons for 'Accounts in this organizational directory only (Crestron Electronics NJ only - Single tenant)' (selected) and 'Accounts in any organizational directory (Any Azure AD directory - Multitenant)'; and 'Advanced settings' with a 'Default client type' dropdown and a 'Treat application as a public client' toggle (set to 'Yes'). A warning message states: 'Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. Learn more about these restrictions.' Below this, a list of supported flows is shown: Resource owner password credential (ROPC), Device code flow, and Integrated Windows Authentication (IWA), each with a 'Learn more' link.

The following authentication settings can be configured for the application:

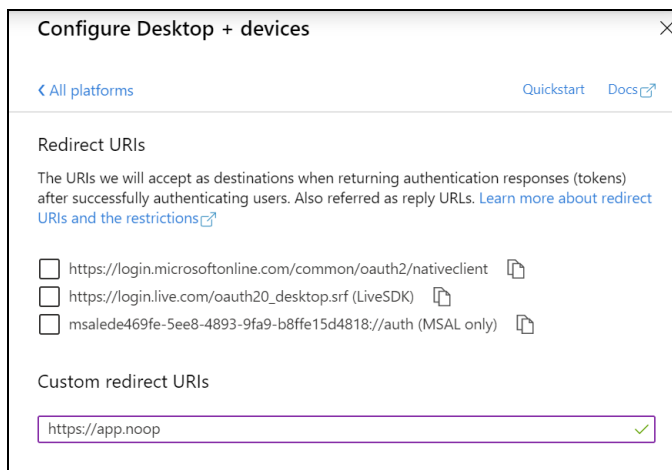
- **+ Add a Platform:** Select this button to create a platform for app authentication. The **Configure platforms** pane is displayed on the right side of the screen.

Configure platforms Pane



Select **Mobile and desktop applications** to display settings for configuring this platform.

Configure Desktop + devices Pane



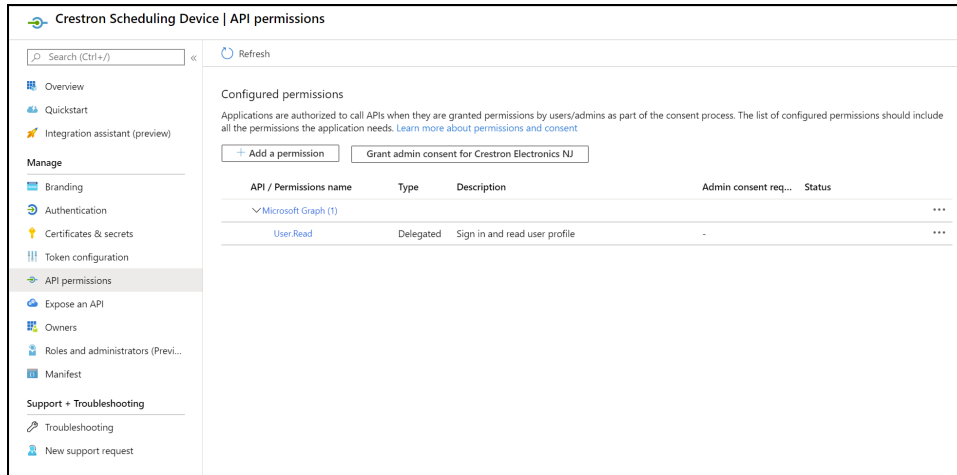
Azure AD requires the use of a redirect URI, but the AirMedia receiver does not. Enter a valid URI address and select **Configure**.

- **Supported account types:** Select an account type for the app. This setting is the same as the one set when registering the app and should not change from **Accounts in this organizational directory only**.
- **Default Client Type:** The **Treat application as a public client** toggle must be set to enabled.

API Permissions

Select **API Permissions** under the **Manage** section of the application navigation menu to configure API permissions for the app.

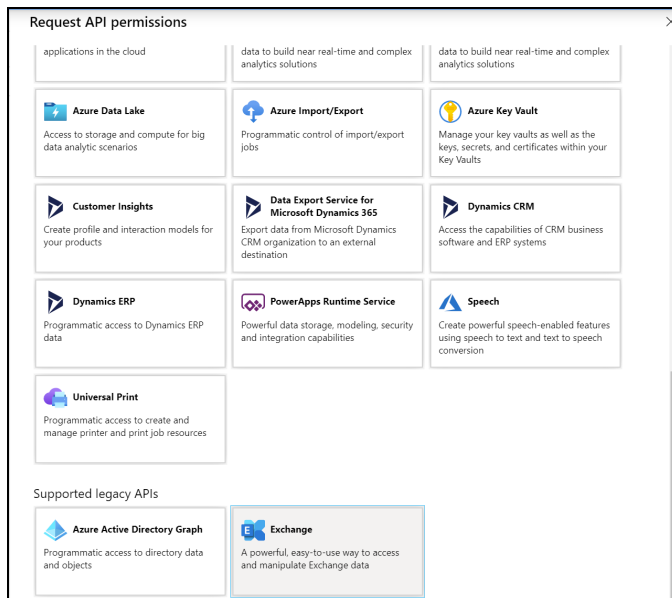
API Permissions Screen



The following API permissions settings can be configured for the application:

Select **+ Add a Permission** to create a new API permission for the app. The **Request API permissions** pane is displayed on the right side of the screen.

Request API permissions Pane



To set the API permissions for EWS:

1. Select **Exchange** to display a list of permissions for EWS.

Request API permissions Pane - Exchange

Request API permissions

< All APIs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions [expand all](#)

Type to search

Permission	Admin consent required
> Calendars	
> Contacts	
> EAS	
▼ EWS (1)	
☒ EWS.AccessAsUser.All Access mailboxes as the signed-in user via Exchange Web Services ⓘ	-
> Exchange	
> Group	
> MailboxSettings	
> Mail	
> Notes	
> People	
> Place	
> Tasks	

[Add permissions](#) [Discard](#)

2. Expand the EWS accordion.
3. Fill the checkbox next to **EWS.AccessAsUser.All** to allow the application to make requests to the Exchange Web Services API on behalf of the configured user.

To set the API permissions for the Microsoft® Graph function:

1. Select **Microsoft Graph** to display a list of permissions for Microsoft Graph.

Request API permissions Pane - Microsoft Graph

Request API permissions

< All APIs

Microsoft Graph
<https://graph.microsoft.com/> [Docs](#) ⓘ

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions [expand all](#)

Type to search

Permission	Admin consent required
☒ email View users' email address ⓘ	-
☒ offline_access Maintain access to data you have given it access to ⓘ	-
☒ openid Sign users in ⓘ	-
☒ profile View users' basic profile ⓘ	-
> AccessReview	
> AdministrativeUnit	
> AgreementAcceptance	
> Agreement	
> Analytics	

[Add permissions](#) [Discard](#)

2. Fill the checkboxes next to the following settings to enable the functionality described below:

- **offline_access:** Allows the application to receive a Refresh Token, which can be exchanged for a new Access Token, when it expires. This is required for long running applications, so user consent is not required each time an access token expires.
- **openid:** Allows the application to receive an ID Token, which provides basic profile information about the authenticated user. This scope is required for the next two scopes, as they are delivered in the ID Token.
- **email:** Provides the email address of the authenticated user. The application uses this to get the calendar address if none is entered during device configuration.
- **profile:** Provides basic profile information about the authenticated user, such as the display name and photo URL.

If the Microsoft Graph **User.Read** scope is added automatically, it can be removed. If there is a warning, it can be ignored.

API Permissions Screen - User.Read Scope

Home > Crestron Electronics NJ | App registrations > Crestron Scheduling Device | API permissions

Crestron Scheduling Device | API permissions

Search (Ctrl+/) Refresh

Remove permission

⚠ This scope is required for proper application functionality.

Are you sure you want to remove Microsoft Graph - User.Read from the configured permissions for Crestron Scheduling Device?

Yes, remove Cancel

Permission	Consent type	Description	State	Actions
EWS.AccessAsUser.All	Delegated	Access mailboxes as the signed-in user via Exchange W...	-	...
Microsoft Graph (5)				...
email	Delegated	View users' email address	-	...
offline_access	Delegated	Maintain access to data you have given it access to	-	...
openid	Delegated	Sign users in	-	...
profile	Delegated	View users' basic profile	-	...
User.Read	Delegated	Sign in and read user profile	-	...

Operation

To present content, use one of the following methods:

- AirMedia wireless presentation
- Connect a device to the HDMI INPUT port (AM-3200(-WF)(-I) models only)

For a description of the receiver's front of room experience, refer to [Front of Room Experience \(below\)](#).

For instructions on using AirMedia wireless presentation, refer to [Present with AirMedia \(on page 89\)](#).

Optionally, a TS- or TSW- 70 series 7 in. or 10 in. touch screen (sold separately) can be used to control the receiver and select which sources are displayed. For instructions on using a touch screen, refer to [Touch Screen Operation \(on page 104\)](#).

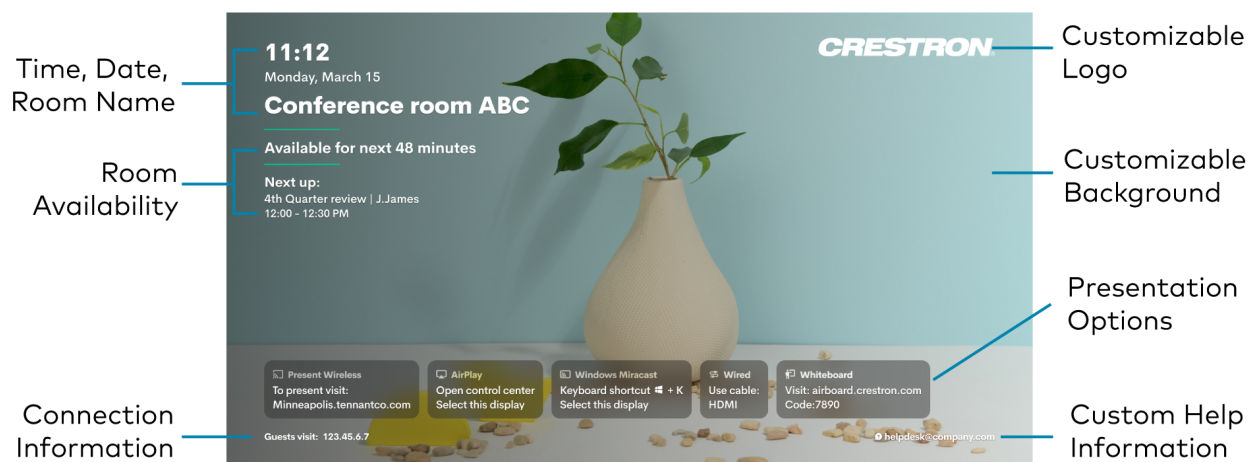
Front of Room Experience

The front of room experience consists of two screens: the welcome screen, which is shown when no users are presenting, and the user presentation screen. The information shown on each screen can be modified using the receiver's web configuration interface.

Welcome Screen

When no users are presenting, the welcome screen is shown on the display device. The welcome screen provides date, time, connection, room availability, and other information as shown in the following image.

Front of Room Experience - Welcome Screen

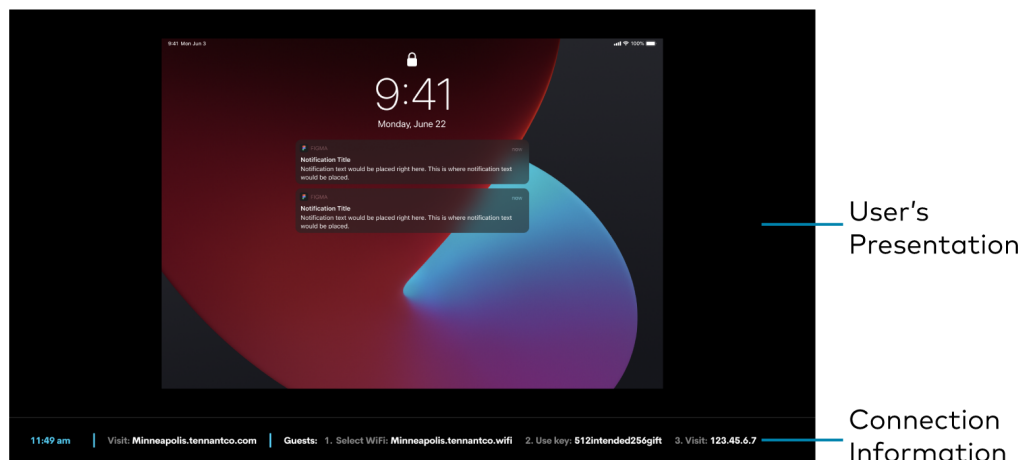


- **Customizable Logo:** Shows the Crestron logo by default. To upload a custom logo, refer to [Connected Devices \(on page 47\)](#).
- **Time, Date, Room Name:** Shows the time, date, and conference room name.
 - **Time/Date:** To configure time and date information, refer to [Date/Time \(on page 35\)](#).
 - **Room Name:** To show, hide, or customize the room name, refer to [General Settings \(on page 25\)](#).
- **Room Availability:** Shows room availability based on the connected calendar. To configure calendar settings, refer to [Services \(on page 38\)](#).
- **Customizable Background:** Shows a slideshow of backgrounds by default. To upload a custom background and/or modify the slideshow settings, refer to [Connected Devices \(on page 47\)](#).
- **Presentation Options:** Shows all of the available ways of sharing content. When a presentation mode is enabled, the presentation option tile will appear on the front of room display. When a presentation mode is disabled, the presentation option tile will not appear. To modify the font size of the of the text in each tile, refer to [Connected Devices \(on page 47\)](#).
- **Connection Information:** Shows additional connection information. To modify what information appears, refer to [Connection Display \(on page 60\)](#).
- **Custom Help Information:** Shows custom help information when configured. To set custom help information, refer to [Connected Devices \(on page 47\)](#).

User Presentation

When a user is presenting, the user's presentation and additional connection information is shown on the display device.

Front of Room Experience Screen - User Presenting



- **User's Presentation:** Shows up to four presentations when AirMedia Canvas is enabled. For more information on Airmedia Canvas, refer to [AirMedia Canvas \(on page 112\)](#). For more information on user presentation, refer to [Operation \(on page 87\)](#).
- **Connection Information:** Shows the time, receiver connection information, and additional connection information. To configure time and date information, refer to [Date/Time \(on page 35\)](#). To modify the connection information shown, refer to [Connection Display \(on page 60\)](#).

Present with AirMedia

The receiver uses a client application to share a Windows or Mac desktop. The computer must be able to access the system over the network.

Crestron offers a standalone application for enterprise deployments. This application features additional connection methods and device management. For details, visit present.crestron.com.

Mobile devices can share their content using the Crestron AirMedia app which is available for iOS and Android™ devices. Both apps may be used for full screen sharing on devices running Android 5.0 Lollipop or iOS 8 and above. Download the latest version of these apps from the App Store® app or Google Play™ store.

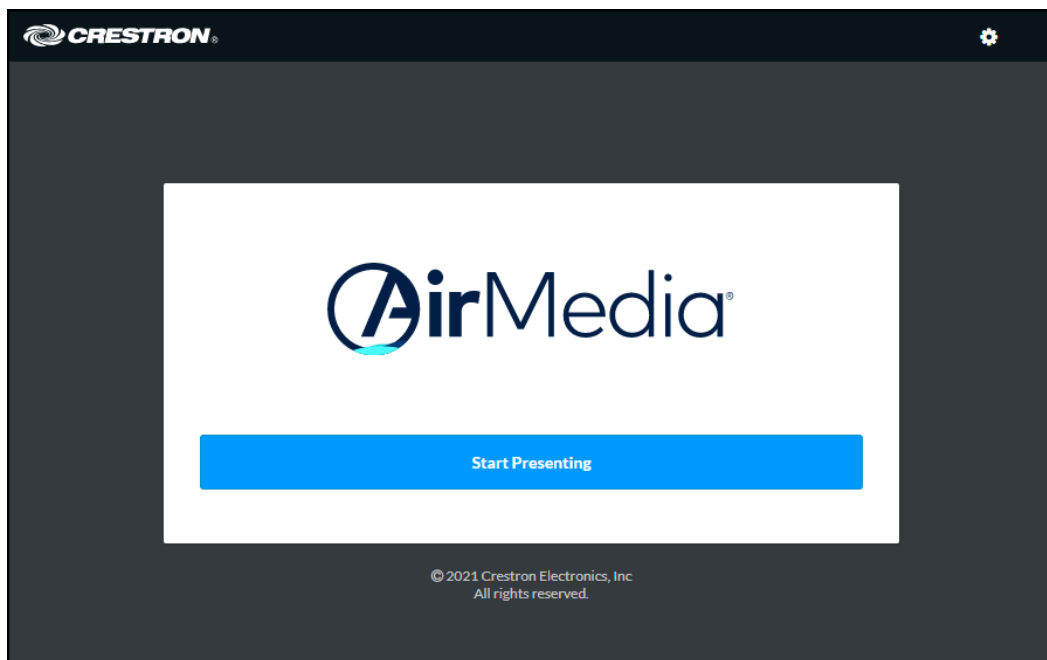
NOTE: For additional details on using AirMedia, refer to the [AirMedia Presentation Gateway Security Reference Guide](#) (Doc 7693).

Establish a Computer Connection

To establish a connection from a computer to a receiver:

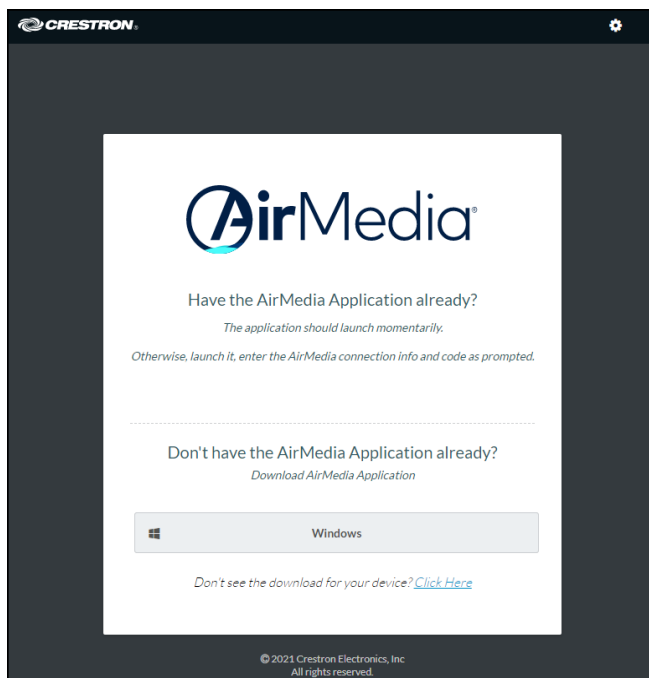
1. Open a web browser on the computer, and navigate to the web address or IP address shown on the display device. The welcome screen is displayed.

Welcome Screen



2. Select **Start Presenting**. The AirMedia screen will display.

AirMedia Screen



3. Select the button for your computer's operating system to download the client application. The client application requires no installation. The application will be downloaded and run locally.

NOTE: When used on a Mac, the AirMedia client application must be run from within the disk image file. Do not drag the application out of the disk image file.

Share Content

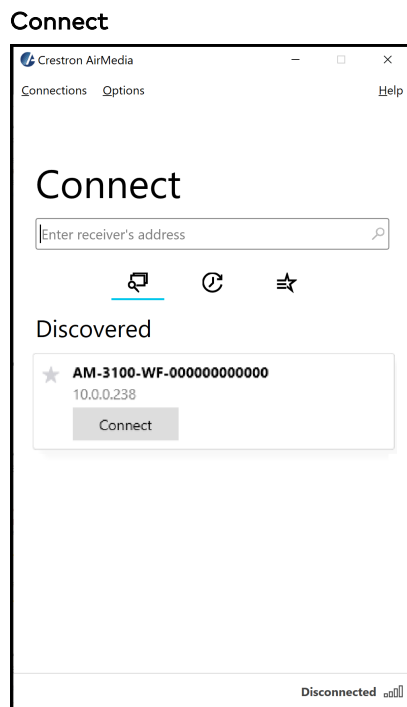
Share content via AirMedia wireless presentation from a Windows computer, a Mac, an iOS device, or an Android device.

From a Windows Computer

Once the client application is downloaded, content can be shared.

To share content from a Windows computer:

1. Run the client application. The **Connect** screen appears and lists any discovered AirMedia devices.

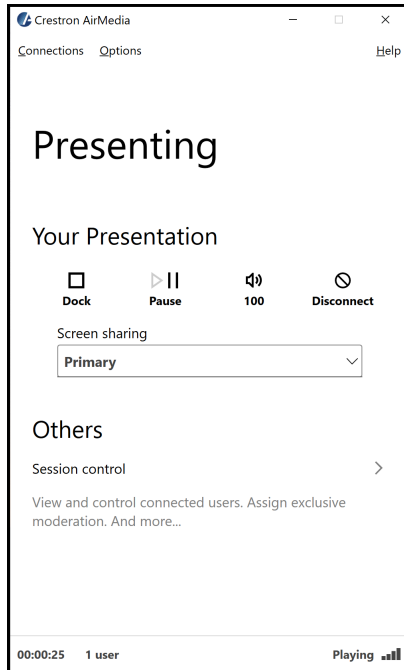


2. Select **Connect** under the desired receiver or enter the device's IP address in the search bar and press enter.

NOTE: Select the star button ★ to the left of the desired receiver to add or remove the receiver from the favorite devices list. Select the favorite devices list button ☆ to access the list.

3. If a code is required, enter the code shown on the display device. Otherwise, the contents of the computer screen will be presented on the display connected to the receiver. Once connected, the client application displays the presentation controls.

Presentation Controls



4. Direct the presentation with the following controls:

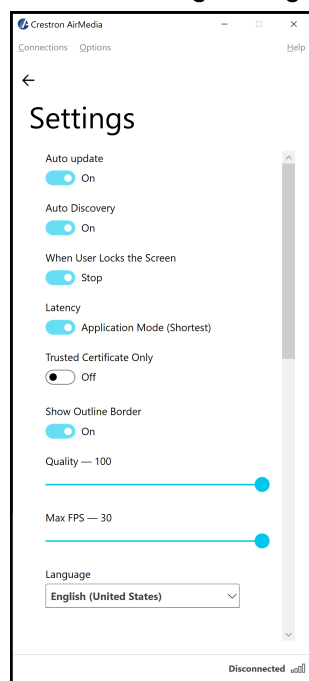
- **Dock**  : Dock the presentation. When docked, the computer no longer shares its screen but remains connected to the receiver.
- **Pause**   : Start or freeze the computer's screen.
- **[Volume]**  : Control the output volume of the display.
- **Disconnect**  : End connection between the computer and the receiver.
- Use the **Screen sharing** dropdown menu to select the connected screen to present.
- Select **Session control** to open the **Session** menu, which lists each presenter along with corresponding presentation controls. Up to 30 presenters can be connected at a time. Use the back arrow to return to the presentation controls for the computer.

NOTES:

- If the computer's presentation is paused and resumed by another presenter, the computer will then receive a permission request before the presentation resumes. To modify this setting, select **Options > Session Delegation**.
- To disable Session control, disable the **Canvas Session Control** setting in the device's web configuration interface. For more information on session control, refer to [AirMedia \(on page 55\)](#).

- Navigate to **Options > Settings** to customize AirMedia settings. Adjust the settings below and select **OK** to save the changes or select **Cancel** to cancel.

AirMedia Settings Dialog Box



- Crestron recommends turning the **Auto Update** toggle to **On**.
- Crestron recommends turning the **Auto Discovery** toggle to **On**.
- **When User Locks the Screen** sets the operation of the client software when a connected computer is locked. Choose from **Stop** (the client stops sharing content), **Pause** (the client pauses sharing content), and **Nothing** (nothing happens).
- **Latency** selects the amount of latency in transmitting the signal from the computer to the receiver. Select **Application Mode (shortest)** for the least amount of latency (best for slides) or **Video Mode (Pre-Buffer)** for a longer amount of latency (best for buffering shared video).
- **Trusted Certificate Only** validates the server certificate before connection
- **Show Outline Border** selects whether or not an orange border appears on the computer's screen when presenting.
- Set the **Quality** of the projected signal (**0** to **100** percent).
- Set the **Max FPS** (frames per second) refresh rate (**1** to **30**).
- Select the **Language** displayed by the client application.

NOTE: The application must be restarted when switching languages.

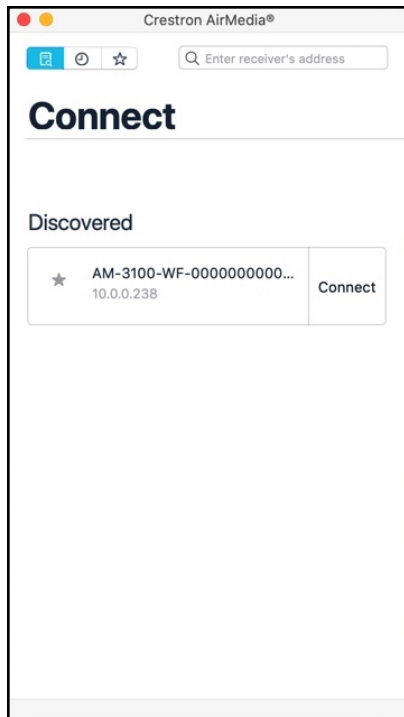
From a Mac

Once the client application is downloaded, content can be shared.

To share content from a Mac:

1. Run the client application. The **Connect** screen appears and lists any discovered AirMedia devices.

Enter Code Dialog Box

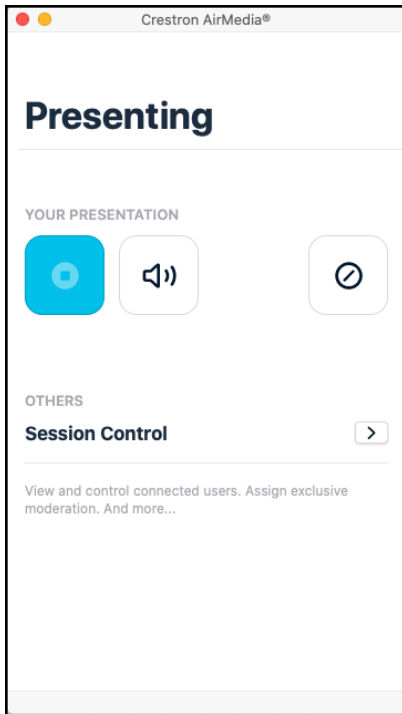


2. Select **Connect** to the right of the desired receiver or enter the device's IP address in the search bar and press enter. The **Enter Code** screen appears.

NOTE: Select the star button ★ to the left of the desired receiver to add or remove the receiver from the favorite devices list. Select the favorite devices list button ☆ to access the list.

3. If a code is required, enter the code shown on the display device. Follow the onscreen instructions to present. Select **OK** to return to the presentation controls.

Presentation Controls



4. Direct the presentation with the following controls:
 - : Dock functionality to be supported in a future release.
 - : Control the output volume of the display.
 - : End the connection between the computer and the receiver.
 - Select **Session control** for additional controls and information about all presenters. The **Session** menu opens and lists each presenter with corresponding presentation controls. Use the back arrow to return to the presentation controls for the computer.

NOTE: To disable Session control, disable the **Canvas Session Control** setting in the device's web configuration interface. For more information on Session control, refer to [AirMedia \(on page 55\)](#).

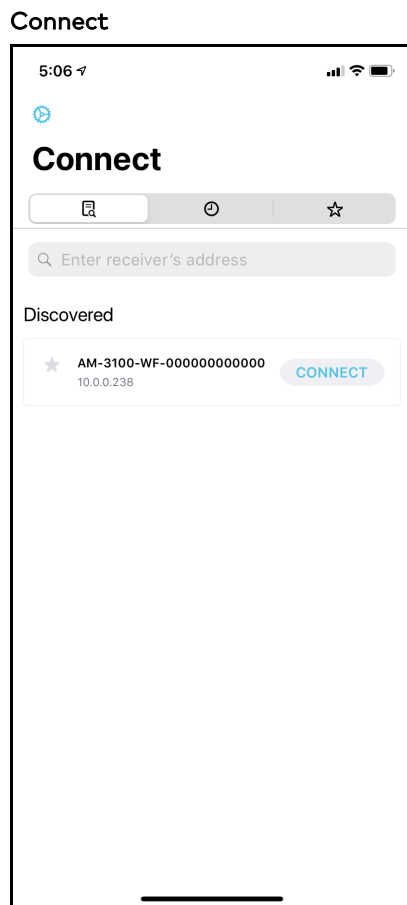
- Select **Options > Settings** in the menu bar to customize AirMedia settings.

From an iOS Device

Content can be shared from an iOS device using the built-in screen mirroring functionality.

To share content from an iOS device:

1. Open the AirMedia application. The **Connect** screen appears and lists any discovered AirMedia devices.



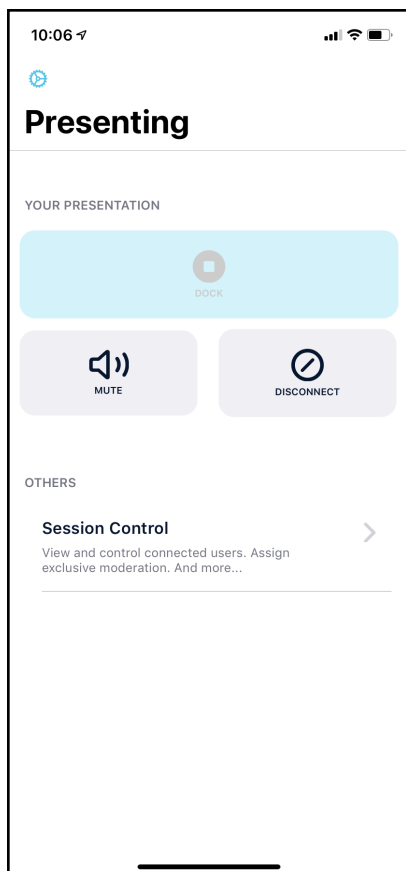
2. Select **Connect** next to the desired receiver or enter the receiver's IP address in the search bar and press **Enter** on the phone's onscreen keyboard.

NOTE: Select the star button ★ to the left of the desired receiver to add or remove the receiver from the favorite devices list. Select the favorite devices list button ★ to access the list.

3. If a code is required, enter the code shown on the display device and select **OK**. Screen mirroring instructions appear.

4. Follow the onscreen instructions and select **OK**. Once connected, the application offers presentation controls.

Presentation Controls



5. Direct the presentation with the following controls:

- **Dock** : Dock functionality to be supported in a future release.
- **Disconnect** : End the connection between the device and the receiver.
- Select **Session control** to open the **Session** menu, which lists each presenter along with corresponding presentation controls. Up to 30 presenters can be connected at a time. Use the back arrow to return to the presentation controls for the device.

NOTE: To disable Session control, disable the **Canvas Session Control** setting in the device's web configuration interface. For more information on Session control, refer to [AirMedia \(on page 55\)](#).

- Tap the settings button in the top left corner to customize AirMedia settings.

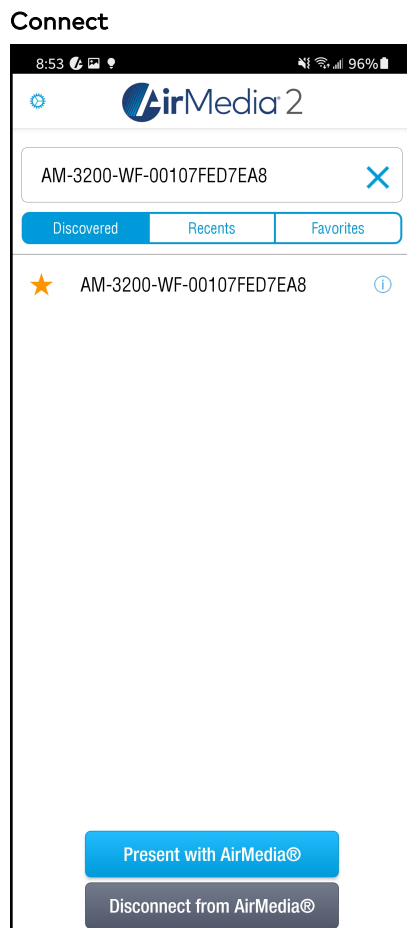
NOTE: If another presenter enters fullscreen mode, presentation from the iOS device will end. The iOS device will remain connected to the receiver. If this occurs, resume the presentation by repeating the screen mirroring instructions described in step 3.

From an Android Device

Content can be shared from an Android device using the AirMedia application.

To share content from an Android device:

1. Open the AirMedia application. The **Connect** screen appears and lists any discovered AirMedia devices.

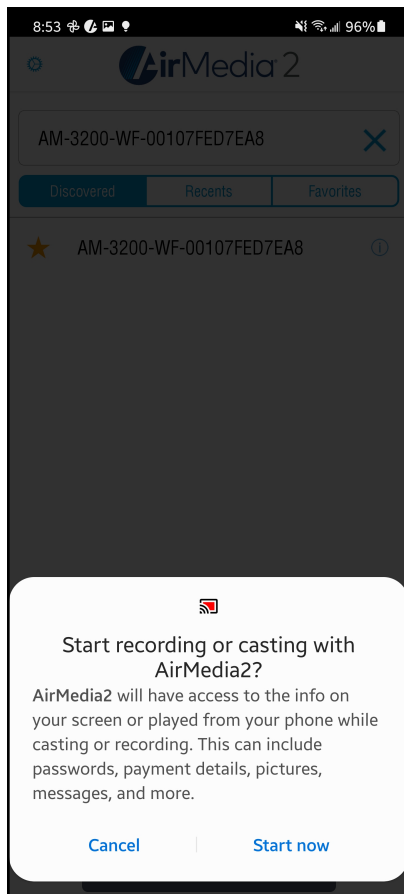


2. Select the desired receiver or enter the receiver's IP address in the search bar and press **Enter** on the phone's onscreen keyboard.

NOTE: Select the star button ★ to the left of the desired receiver to add or remove the receiver from the favorite devices list. Select **Favorites** to access the list.

3. If a code is required, enter the code shown on the display device and select **OK**. A presentation confirmation message appears.

Presentation Confirmation

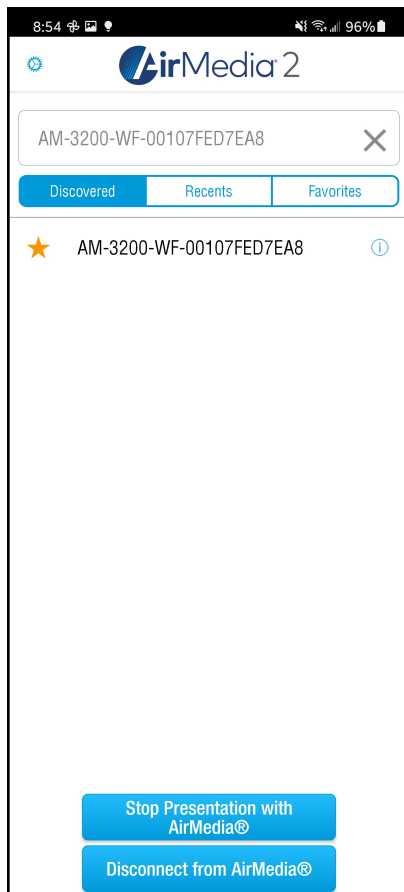


4. Select **Start now** to begin presenting.

To end the presentation, make one of the following selections:

- **Stop Presentation with AirMedia:** Stop presenting from the Android device but remain connected to the receiver.
- **Disconnect from AirMedia:** Stop presenting from the Android device and disconnect from the receiver.

Presentation Screen



Using Miracast

Miracast is a mirroring protocol and wireless technology used to project your screen to the receiver without the need to install an application on your Windows computer.

To present using Miracast with an AirMedia receiver:

1. Open the Windows connect menu via the Windows notification center or via the shortcut  (Windows) + K. On touch-capable Windows 10 devices, swipe in from the right edge of the screen.
2. Select the desired receiver from the list.
3. If a code is required, enter the code shown on the display device.

For more details on using Miracast with the AirMedia receiver, refer to the [AirMedia Presentation Gateway Security Reference guide](#) (Doc 7693).

Touch Screen Operation

A connected touch screen running .AV Framework software can be used to control presentations. Use the touch screen to control volume, switch between sources, and start and stop presentations. The home screen is displayed when the system starts.

Add a Touch Screen

The receivers support the use of a TS- or TSW- 70 series 7 in. or 10 in. touch screen for system control. Adding a touch screen to the system requires an entry in the touch screen's IP table and loading a touch screen project file to the touch screen.

NOTE: The touch screen must be accessible to the receiver over the network.

IP Table Entry

An IP table entry must be created to direct the touch screen to the IP address or host name of the receiver. For instructions on creating an IP table entry, refer to the touch screen's product manual:

- [TSW-570, TSW-770, and TSW-1070 Product Manual](#) (Doc. 8550)
- [TS-770 and TS-1070 Product Manual](#) (Doc. 8555)

Load a Touch Screen Project File

If internet connectivity is available on the receiver, the system automatically loads the touch screen project file once the IP table entry is complete. To automatically load the touch screen project file, touch screen auto update must be enabled as described in [Connected Devices \(on page 47\)](#).

To download the touch screen project file, refer to the receiver's product page:

- [AM-3100-WF](#)
- [AM-3100-WF-I](#)
- [AM-3200](#)
- [AM-3200-WF](#)
- [AM-3200-WF-I](#)

For details on manually loading a touch screen project file, refer to the touch screen's product manual:

- [TSW-570, TSW-770, and TSW-1070 Product Manual](#) (Doc. 8550)
- [TS-770 and TS-1070 Product Manual](#) (Doc. 8555)

Screen Controls

When connected, the touch screen will display the home screen.

Home Screen



The footer bar provides the same buttons regardless of which screen is selected. Refer to the following tables for more information on footer button functionality.

Footer Buttons

	The more button navigates to the selection screen.
	The info button navigates to the information screen.
	The volume lower button lowers the device volume incrementally.
	The volume raise button raises the device volume incrementally.

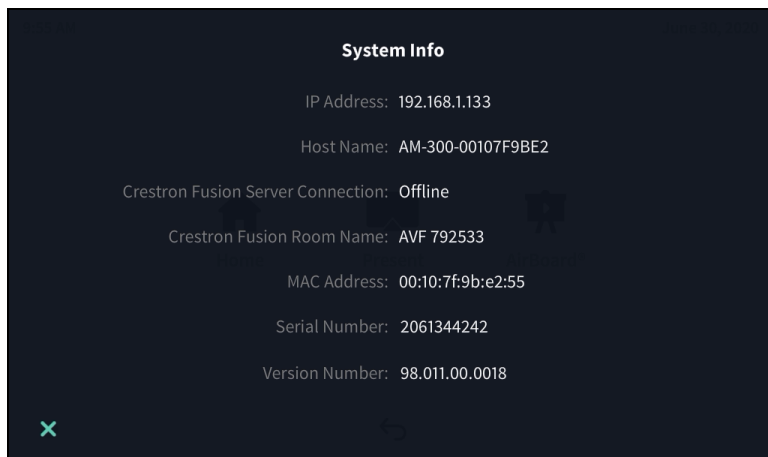
NOTE: Volume controls are only present when the system is connected to a display device that supports volume control.

Access the System Info Screen

To access the **System Info** screen, tap and hold the information button  on the home screen for 20 seconds.

The **System Info** screen provides the device IP address, the device hostname, the Crestron Fusion server connection status, the Crestron Fusion room name, the device MAC address, the device serial number, and the .AV Framework version number.

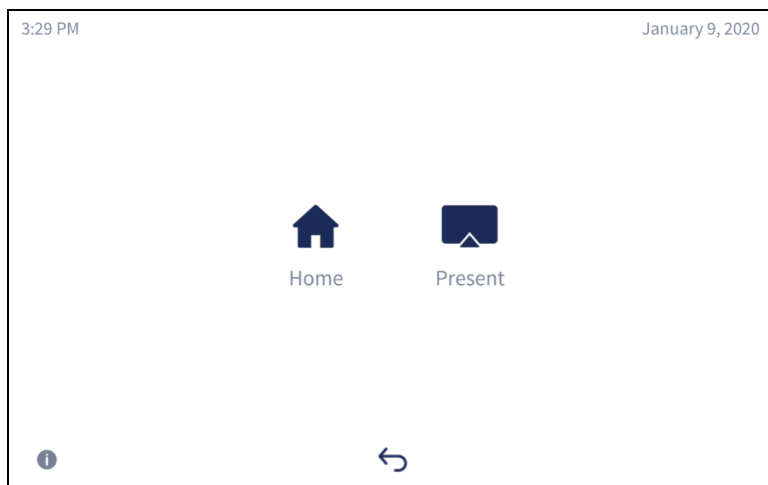
System Info screen



The Function Menu

Tap the more button  on the home screen to display the function menu.

Function Menu



- Tap **Home** 🏠 to display the Home screen.
- Tap **Present** 🖥️ to view presentation options. For details, refer to [Present a Source \(on page 110\)](#).
- Tap the back button ⬅️ to return to the previous screen

Room Scheduling

The Home screen is used to reserve the conference room.

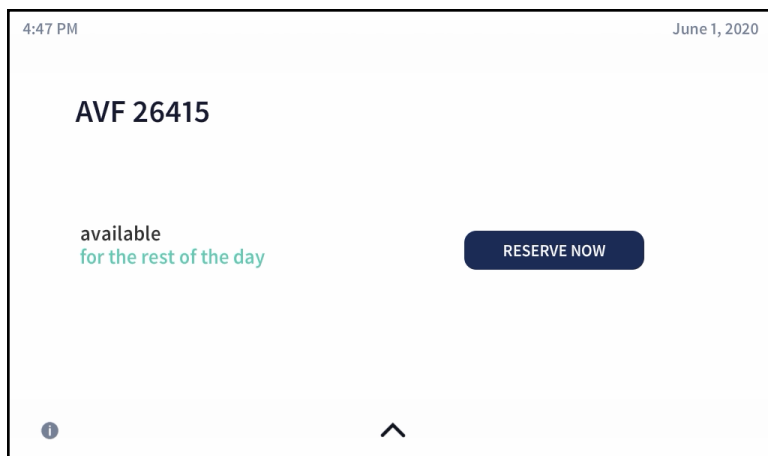
Tap **Home** 🏠 to display the home screen. The home screen displays the current status of the room.

Room Available

If the room is available for use, the touch screen provides the following information:

- The time remaining (in minutes) until the next scheduled meeting occurs
- A **RESERVE NOW** button that allows an ad hoc meeting to be scheduled through the touch screen

Home Screen – Available Room



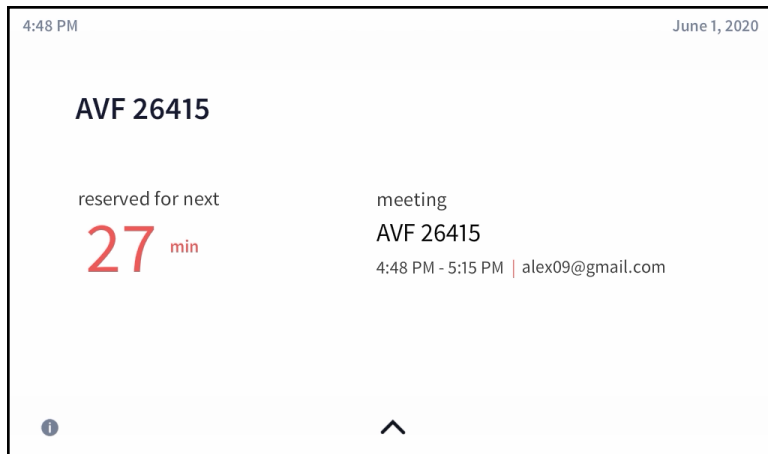
Room Reserved

If the room is not available, the home screen provides the following information:

- The time remaining (in minutes) until the current meeting ends
- The duration, name, and organizer of the scheduled meeting

You can use the room for the remaining time available or reserve the room for another time.

Home Screen – Reserved Room



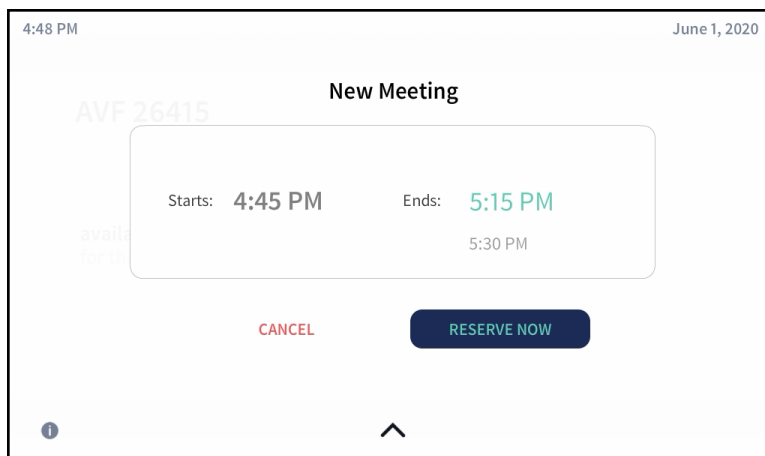
Reserve the Room

To reserve an ad hoc meeting from the home screen when the room is available:

1. Tap **RESERVE NOW** on the home screen. The **New Meeting** screen is displayed.

NOTE: RESERVE NOW meetings may only be scheduled for the current day.

New Meeting Screen



2. Tap one of the available meeting end times to set the duration of the meeting. The room can be reserved for up to three lengths:
 - Until the current half hour interval ends (If the current time is 4:44 pm, the end time for this option is 5:00 pm.) This is the default setting.
 - Until the current half hour interval ends plus 30 minutes (If the current time is 4:44 pm, the end time for this option is 5:30 pm.)
 - Until the current half hour interval ends plus 60 minutes (If the current time is 4:44 pm, the end time for this option is 6:00 pm.)

NOTE: These options are available only if a meeting is not already scheduled during these times.

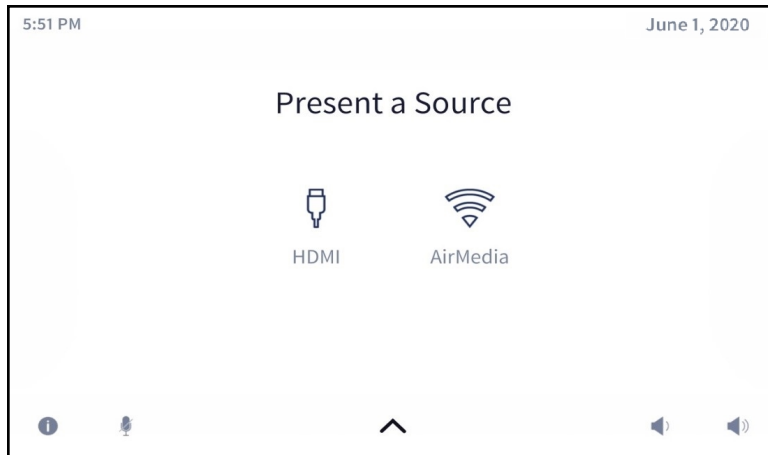
3. Tap **RESERVE NOW** to reserve the meeting.

To discard the reservation, tap **CANCEL**.

Present a Source

To present a connected source, tap **Present**  from the function menu. The **Present a Source** screen appears. The **Present a Source** screen allows content to be routed from a connected device to the main display in the room.

Present a Source Screen



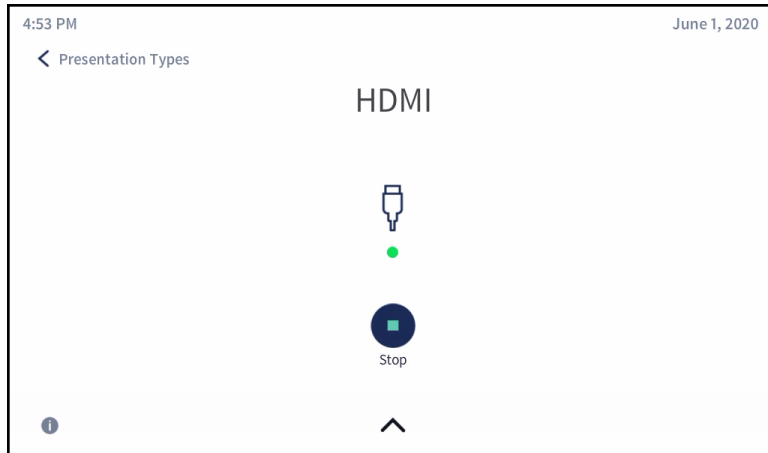
To present content from a source device, select one of the available presentation options. The source is controlled directly through the touch screen.

If a source is active, a **Stop**  button is shown. Tap the **Stop**  button to stop routing the source to the display.

Present via HDMI

To display content from a source connected via HDMI, tap **HDMI** . The following screen will appear.

Present Screen - HDMI Source



The dot in the center of the screen turns green if the source is connected and turns red if the source is disconnected.

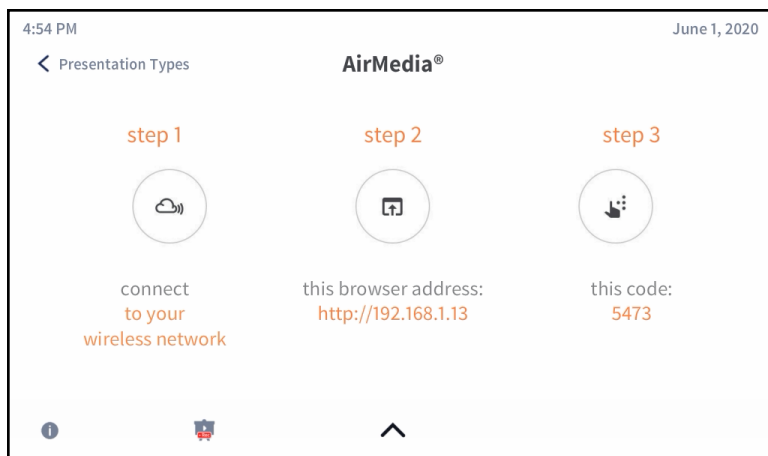
When done presenting, tap **Stop** .

To return to the previous screen, tap **< Presentation Types**. Tapping **< Presentation Types** does not disconnect the source.

Present via AirMedia

Tap **Wireless** to display content from a device connected through AirMedia. The **AirMedia®** screen is displayed with instructions to present with AirMedia.

AirMedia® Screen



Refer to [Control Multiple Sources \(on the facing page\)](#) for instructions on controlling an AirMedia presentation from the touch screen.

Refer to [Present with AirMedia \(on page 89\)](#) for instructions on connecting to AirMedia and sharing content.

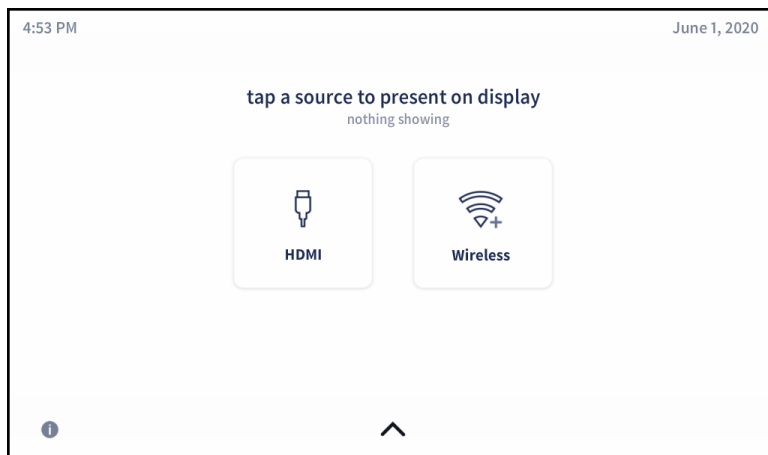
AirMedia Canvas

When configured, the receiver can show multiple sources on the display device simultaneously. The touch screen is used to manage the sources shown on the display device.

NOTE: For details on configuring the receiver to use the AirMedia Canvas feature, refer to [AirMedia \(on page 55\)](#).

When AirMedia Canvas and Canvas Session Controls are enabled, the Present a Source screen appears as shown below.

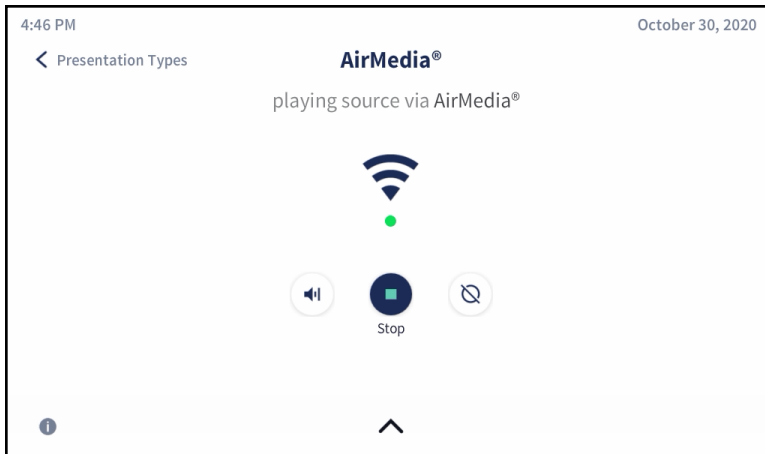
Present a Source Screen



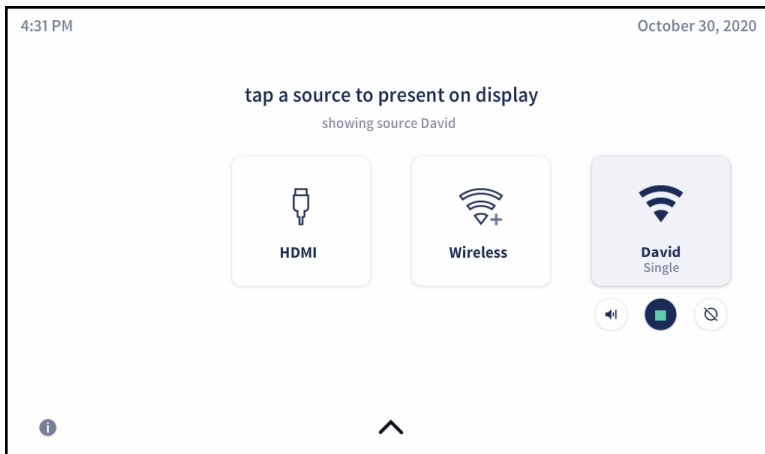
Control Multiple Sources

To control multiple sources using Canvas Session Controls:

1. Connect all sources to the receiver.
2. Tap the first source for presentation. The content will appear on the display device with presentation controls.
 - Select the volume button  to mute or unmute the source's volume.
 - Select **Stop**  to dock the presentation. When docked, the source stops presenting but remains connected to the display. Select the play button  to resume presenting. When resuming a presentation, a permission request is sent to the source device. The request must be accepted before the presentation resumes.
 - Select the disconnect button  to disconnect the source from the receiver.

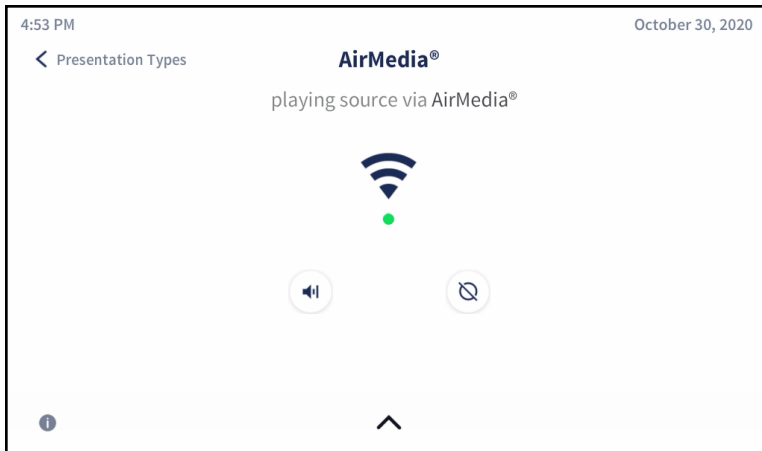


3. Tap < **Presentation Types**. The touch screen will show the connected source with the presentation controls detailed in the previous step.

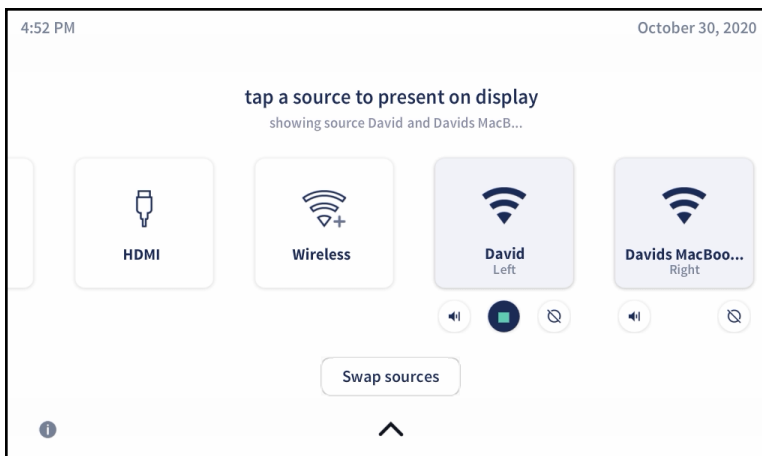


4. Tap the second source for presentation. The display device will show the two sources side by side.

NOTE: The dock control feature will be implemented for Apple® devices in a future release. Select the disconnect button  to end the presentation and disconnect the source device.



5. Tap < **Presentation Types**. The touch screen will show the two connected sources side by side.



6. (Optional) Tap more sources to present as needed. The touch screen will show all connected sources side by side, and the presentations will be arranged on the display device.

NOTE: If the maximum amount of presenters is reached and another source is selected, then the first source will be docked (AirMedia user) or disconnected (hard wired inputs, AirPlay connection, or Miracast connection) and the latest source will take its place on the display. When docked, the source stops presenting but remains connected to the display. To adjust the maximum amount of sources that can present simultaneously, refer to [General Settings \(on page 56\)](#)

Switch to Single Source

When two sources are shown on the display device, tap **Stop**  to remove the source's presentation from the display device. The remaining source will be presented in full screen.

Swap Sources

When two sources are shown on the display device, tap **Swap Sources** to switch the positions of two sources.

When more than two sources are shown on the display device, the **Swap Sources** button is unavailable.

This page is intentionally left blank.

