



AM-200/AM-300 AirMedia® 2.0 Presentation Systems

Product Manual
Crestron Electronics, Inc.

Regulatory Models: AM-200 and AM-300

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: AM-200, AM-300

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, Crestron AirBoard, AirMedia, .AV Framework, Crestron Connected, Crestron Fusion, Crestron Studio, Crestron Toolbox, DigitalMedia, DM, Pinpoint, XiO Cloud, and Zūm are either trademarks or registered trademarks of Crestron Electronics, Inc. in the United States and/or other countries. App Store, AirPlay, iPad, iPhone, iTunes, and Mac 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 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 and the HDMI logo are either trademarks or registered trademarks of HDMI Licensing LLC in the United States and/or other countries. Active Directory, Azure, Microsoft, Microsoft 365, Microsoft Exchange Server, Outlook, PowerShell, and Windows are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. 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.

HDMI

©2020 Crestron Electronics, Inc.

Contents

Introduction	1
Requirements	5
Administrator	5
Operating Environment	5
Configuration	7
Requirements	7
Connect to the Device	7
Log Out from the Device	12
Configure the Device	12
HDMI INPUT	12
DM IN (AM-300 Only)	16
HDMI OUTPUT	19
NETWORK	20
DEVICE	32
APPSPACE	44
AMPS	45
AirMedia	93
Crestron AirBoard	102
Enterprise Deployment Options	106
XiO Cloud Service	106
Claim a Single Device	106
Claim Multiple Devices	108
Crestron Deployment Tool for PowerShell® Software	109
Operation	110
Connect a Source	110
Touch Screen Operation	110
Touch Screen Controls	111
Screen Controls	111
Schedule a Meeting	113
Present Content	116
AirMedia Canvas	123
Keypad Operation	126
System Power	126
Volume	126
Use AirMedia	126
Establish a Connection	127

Share Content	128
Appendix A: Enabling Modern Authentication for EWS	131
Create the Application	131
Obtain Authentication IDs	133
Configure Additional Settings	134
Appendix B: AM-200 and AM-300 Systems	141
Hookup Diagrams	141
Supported and Tested DigitalMedia Transmitters (AM-300 Only)	142
Zūm® Devices	142
Supported Devices	143
Add a Zūm Device to the Network	143
Monitor and Test Zūm Devices	144
Add a Touch Screen	144
IP Table Entry	144
Load a Touch Screen Project File	144

Introduction

The AM-200 and AM-300 AirMedia® Presentation Systems provide room scheduling, and wired and wireless presenting capabilities for smaller conference rooms and huddle spaces. For more information on features, capabilities, and specifications on the AM-200 and AM-300, visit their respective websites at www.crestron.com.

Feature Comparison

FEATURE	AM-101	AM-200	AM-300
AirMedia 2.0 technology	x	✓	✓
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™ ¹ operating system	x	✓	✓
Mac devices	✓	✓	✓

¹The 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 framerate) 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).

FEATURE	AM-101	AM-200	AM-300
AirMedia Video + Audio Playback (continued)			
iPad devices	✓	✓	✓
iPhone devices	✓	✓	✓
iOS devices	✓	✓	✓
Android devices	✗	✗	✗
AirMedia Playback Features			
DRM Content Support (Netflix, etc.)	✗	✗	✗
Device Internet Connection Required for AirPlay® Mirroring	✗	✓	✓
Security			
AES-128/TLS security	✗	✓	✓
802.1X	✗	✓	✓
Active Directory® Authentication	✗	✓	✓
Crestron® Control			
.AV Framework™ Platform	✓	✓	✓
XiO Cloud® Service	✗	✓	✓
Crestron Studio® Software	✓	N/A	N/A
SIMPL Windows	✓	✓	✓
SIMPL#	✓	✓	✓
Virtual Control	✓	✓	✓
Video Inputs			
HDMI® Input	✗	1	1
HDMI Resolution	✗	1080p	1080p
HDMI HDCP	✗	HDCP 1.4	HDCP 1.4
4K DigitalMedia™ Input	✗	✗	1
4K DigitalMedia Resolution	✗	✗	4k60 4:2:0
4K DigitalMedia HDCP	✗	✗	HDCP 2.2
Video Outputs			
HDMI Output	1	1	1 – 4K
HDMI Resolution	1080p	1080p	4K30
HDMI HDCP	HDCP 1.4	HDCP 1.4	HDCP 2.2

FEATURE	AM-101	AM-200	AM-300
Touch Screen Support	Via programming only	External	External
Zūm® Sensors and/or Buttons	x	✓	✓
PoE Occupancy Sensor (CEN-ODT-C-POE)	x	✓	✓
Other Interfaces			
COM/IR Support	x	✓	✓
CEC	x	✓	✓
Power Over Ethernet	x	✓	x
Direct Connect Scheduling Integration ¹			
Microsoft Exchange Server® or Microsoft 365®	x	✓	✓
Google Calendar™	x	✓	✓
General Features			
Appspace® Application	x	✓	✓
Crestron AirBoard™ Whiteboard Capture System	x	✓	✓
AirMedia Canvas	x	✓	✓
Quad View	✓	x	x
Remote View	✓	x	x
Moderator Mode	Windows & Android	x	x
Control System Interface	✓	✓	✓
AM-101 Compatibility Mode	N/A	✓	x
YouTube® software Pushmode Support	x	✓	✓
Mounting	Freestanding Surface	Freestanding Surface Rack	Freestanding Surface Rack
Dimensions (W x H x D)	6.15 in. x 1.10 in. x 2.39 in.	7.40 in. x 6.42 in. x 1.35 in.	9.29 in. x 7.93 in. x 1.36 in.

¹Connection via Crestron Fusion® software may allow additional providers.

This product manual discusses the requirements, configuration instructions, and operating instructions for the AM-200 and AM-300. For information on installing the AM-200, refer to the [AM-200 DO Guide](#) (Doc. 8260). For information on installing the AM-300, refer to the [AM-300 DO Guide](#) (Doc. 8253).

Requirements

Administrator

This document is written for use by a facility's Information Technology (IT) administrator. The IT administrator should have the following knowledge and skills:

- General Skills
 - IP Networking
 - Basic PC Operation and Administration
 - Calendaring system administration (for calendar connectivity)
- Crestron-specific skills
 - Crestron Fusion® monitoring and scheduling software helps an administrator organize and display room availability, collect data on room usage, and monitor devices on a network. For training, visit <https://www.crestron.com/trainingonlinecourse?id=14>.

NOTE: You must be logged in to your Crestron.com account to access the training course.

- XiO Cloud® service (Cloud Provisioning) helps an administrator quickly manage all of the devices within an environment. The platform allows an administrator to add devices to a system in order to manage their status, change settings, update firmware, set up new users, manage access levels and manage automated alerts. For training, visit <https://www.crestron.com/en-US/Support/Tools/Applications/Training-Online-Course?id=31>.

NOTE: You must be logged in to your Crestron.com account to access the training course.

Operating Environment

The AM-200 and AM-300 require the following to make the most of their capabilities.

- Zūm® devices for control and occupancy sensing. The following devices can be used with an AM-200 or AM-300.
 - [ZUMMESH-AVBRIDGE](#) or [ZUMMESH-AVBRIDGE-I](#) Wireless Control Integration Module to connect Zūm® devices to the AM-200 or AM-300.
 - [ZUMMESH-KP10AMBATT](#) AirMedia keypad for system control.

- [ZUMMESH-PIR-OCCUPANCY-BATT](#) Wireless Battery-Powered Occupancy Sensor to automatically control the power of a display device based on room occupancy and events.

For details on configuring and using Zūm devices as part of an AM-200 or AM-300 system, refer to [Zūm® Devices \(on page 142\)](#).

- A PoE occupancy sensor (as an alternative to the ZUMMESH-PIR-OCCUPANCY-BATT occupancy sensor) to automatically control the power of a display device based on room occupancy and events. The [CEN-ODT-C-POE](#) can be used with an AM-200 or AM-300.

For details on configuring and using a PoE occupancy sensor as part of an AM-200 or AM-300 system, refer to [Device Configuration \(on page 88\)](#).

- A TSW touch screen for system control.

For details on configuring and using a touch screen as part of an AM-200 or AM-300 system, refer to [Add a Touch Screen \(on page 144\)](#).

- An HDMI source with HDMI cable or a Crestron AirBoard™ Whiteboard Capture System (model [CCS-WB-1](#)) for presentation.

For details on using an HDMI connected device as part of an AM-200 or AM-300 system, refer to [Present Via HDMI \(on page 117\)](#).

For details on using a Crestron AirBoard device as part of an AM-200 or AM-300 system, refer to [Present from the Crestron AirBoard Whiteboard Capture System \(on page 118\)](#).

- Crestron Fusion software to monitor and manage an AM-200 or AM-300 from a central location. When used with an optional occupancy sensor, Crestron Fusion software also supports room scheduling and provides the ability to integrate with many third-party calendaring applications. Crestron Fusion software can also send pop-up messages that can display prominently on the display device in the event of an emergency or other important announcement.
- An XiO Cloud license to monitor and manage the AM-200 or AM-300 from a central location using Crestron's XiO Cloud service.
- Microsoft Exchange Server, Microsoft 365, or Google Calendar calendaring applications to allow space availability and calendar event details to appear on the display device.

Configuration

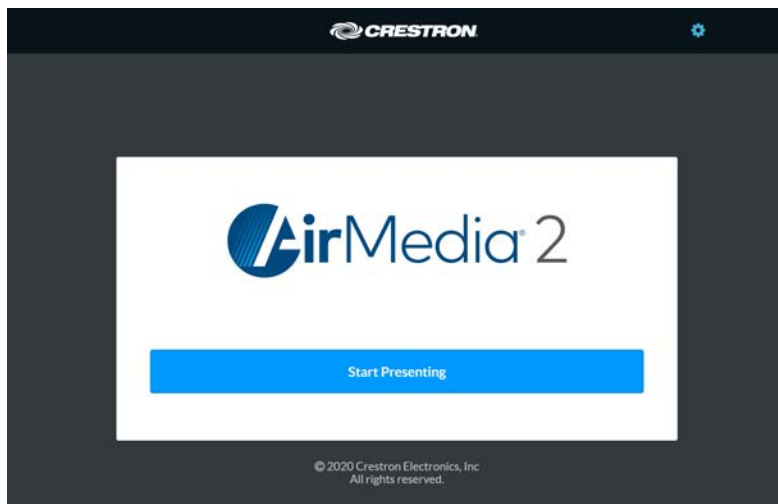
Requirements

Configuration requires a computer with web browser software. The computer must be connected to the same network as the AM-200 or AM-300.

Connect to the Device

1. On the 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.

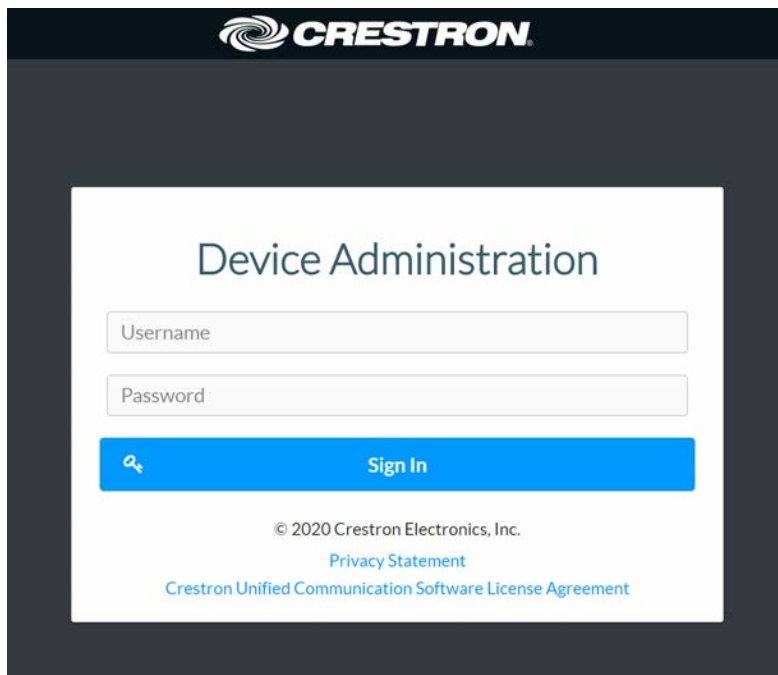
Welcome Screen



2. Click  to continue. A login screen is displayed.

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 correct IP address or host name of the device.

Login Screen



3. Enter the default user name ("admin") and password ("admin"), and click **Sign In** to continue. The device's **Status** screen is displayed.

If this is a brand new device, or the device has been restored to factory settings, a prompt to enter a new user name and password will be displayed.

Enter New User Name and Password

CRESTRON

⚠ DEVICE FIRST BOOT

Device Administration

Username

Password

Confirm Password

+ Create User

© 2020 Crestron Electronics, Inc.
[Privacy Statement](#)
[Crestron Software End-User License Agreement](#)

Enter the new user name and password in their respective fields and click **Create User**. The device's **Status** screen is displayed.

Status Screen

CRESTRON

STATUS

- HDMI INPUT
- DM IN
- HDMI OUTPUT
- NETWORK
- DEVICE
- APPSPACE
- AMPS
- AIRMEDIA
- AIRBOARD

General

Model AM-300
Firmware Version 1.4493.00020
Serial Number 2061344

+ Show More

Network

Control System Connections

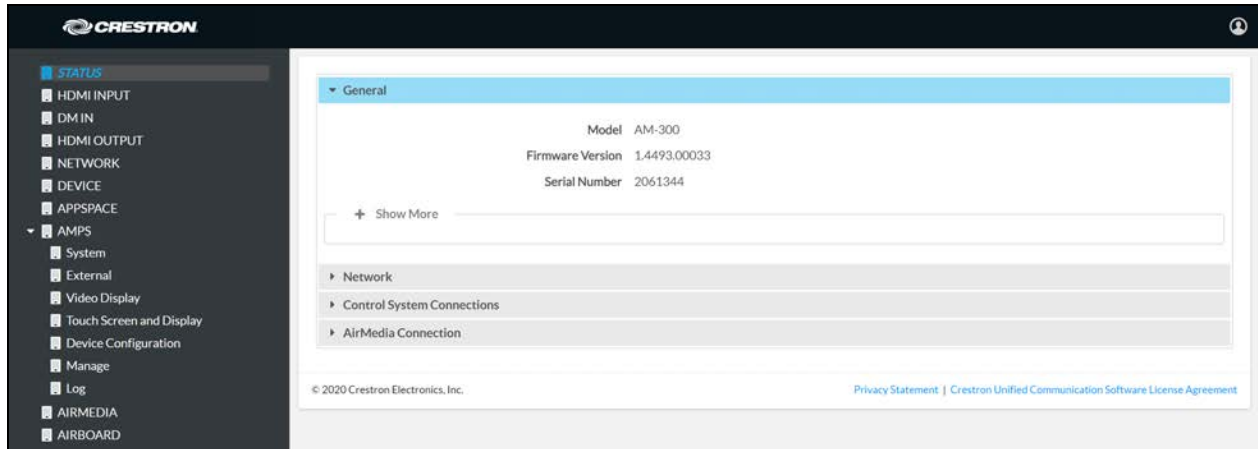
AirMedia Connection

© 2020 Crestron Electronics, Inc. [Privacy Statement](#) | [Crestron Unified Communication Software License Agreement](#)

The **Status** screen displays information about the device and allows configuration of the device's operating parameters:

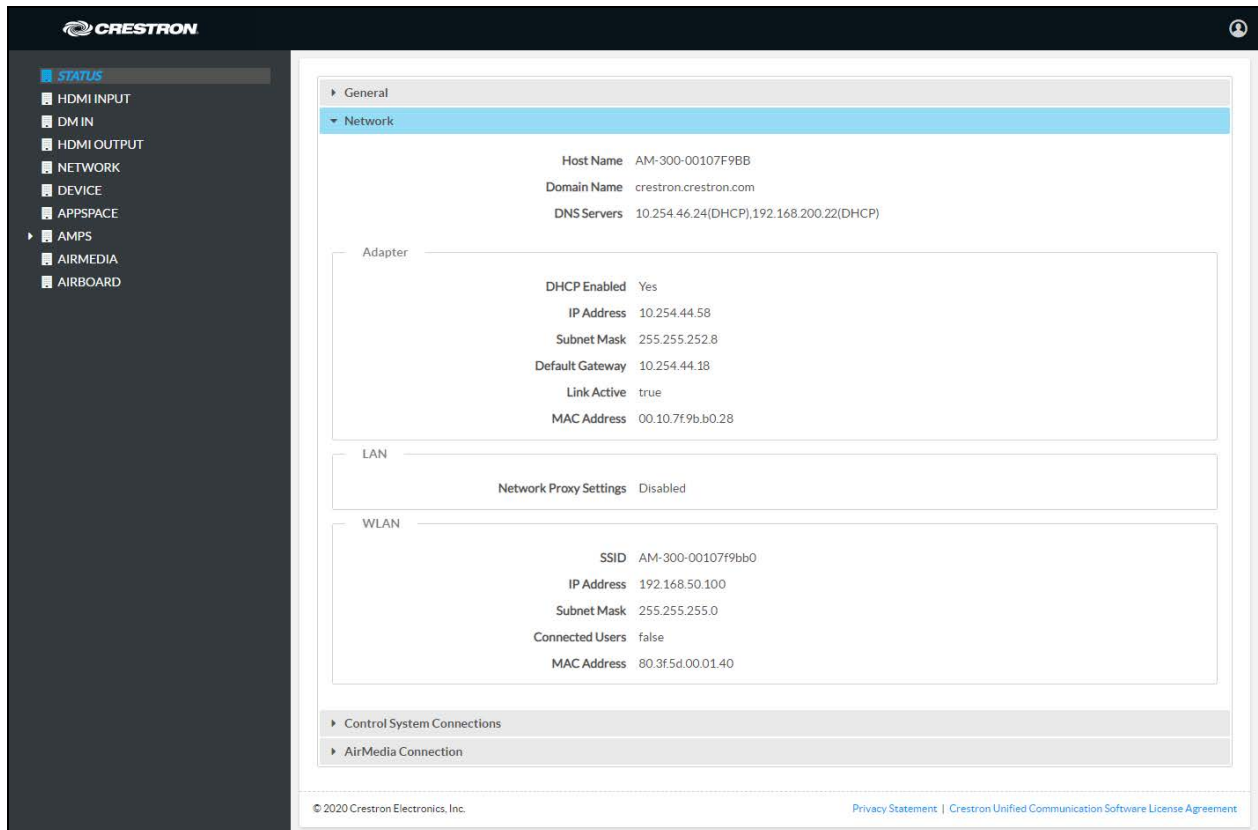
- **STATUS** contains general information about the device, network information, control system connections, and the AirMedia connection.
 - Click **General** to view general information.

Status Screen – General



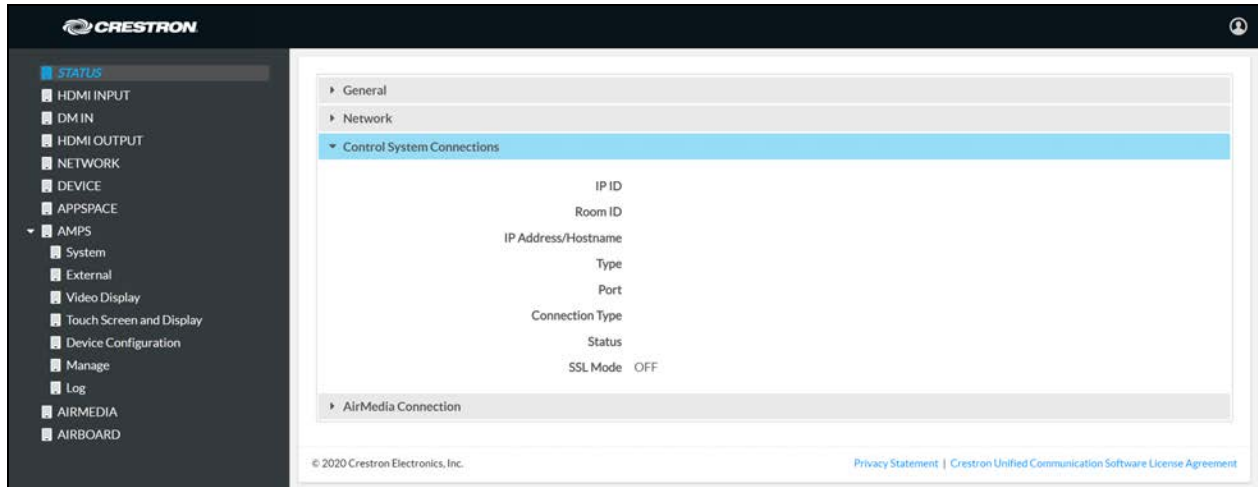
- Click **Network** to view network information.

Status Screen – Network



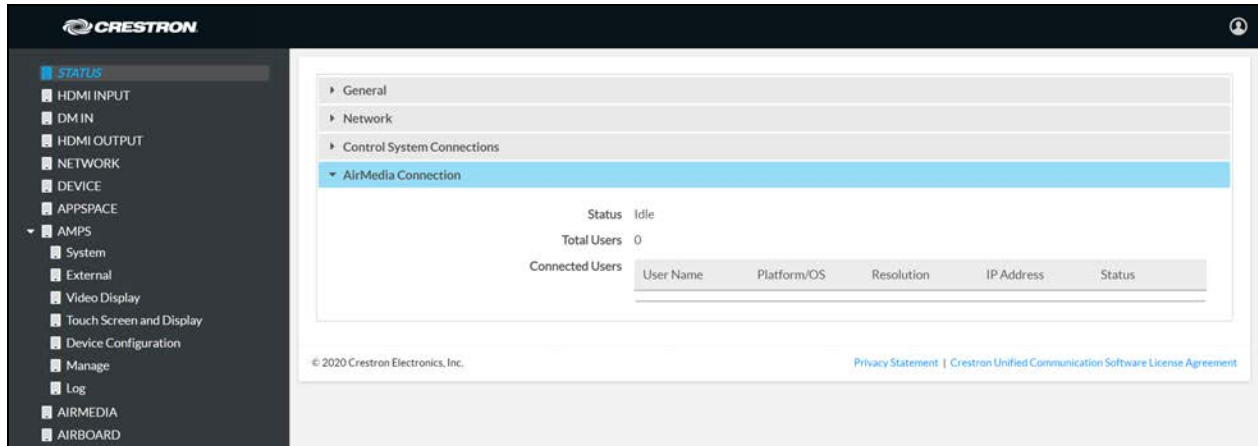
- Click **Control System Connections** to view information about the device's connection to a control system.

Status Screen – Control System Connections



- Click **AirMedia Connection** to view information about the AirMedia connection.

Status Screen – AirMedia Connection




- **HDMI INPUT** configures the HDMI input.
- **DM IN** configures the DM® input (AM-300 only).
- **HDMI OUTPUT** configures the HDMI output.
- **NETWORK** configures the device for operation in a network environment.
- **DEVICE** is used for device management, enabling automatic firmware updates, configuring the control system connection, setting the date and time, and authentication management.
- **APPSPACE** is used to configure the device to work with the Appspace content management application for digital signage.

- **AMPS** configures system settings, Crestron Fusion software operation, the display device, touch screen operation, and the Zūm network. It also manages the system's configuration, and allows viewing of activity logs.
- **AIRMEDIA** configures the device's AirMedia presentation gateway.
- **AIRBOARD** configures the device's functionality with a CCS-WB-1 Crestron AirBoard™ Whiteboard Capture System.

When displayed on any screen, click **+ Show More** to view more details or click **- Show Less** to view fewer details.

Log Out from the Device

Click  to log out from the device and return to the welcome screen.

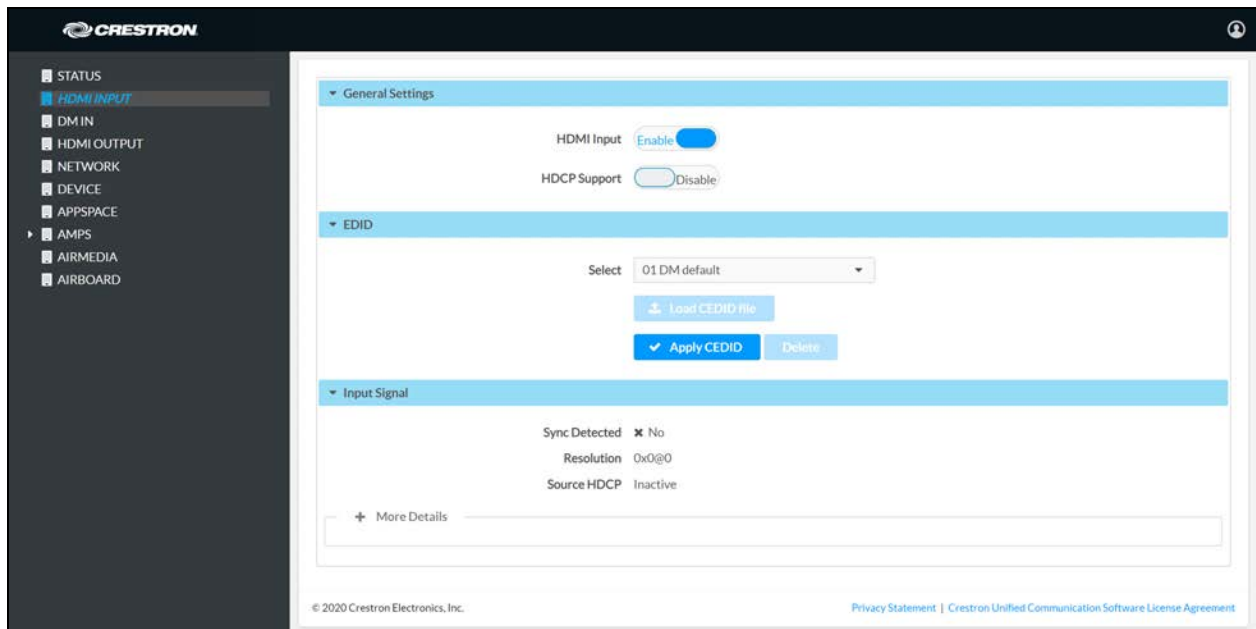
Configure the Device

Configure the device as required for the installation.

HDMI INPUT

Click **HDMI INPUT** to configure the HDMI input. The screen displays controls for HDCP support and EDID, as well as information about the input signal (if present).

HDMI INPUT Screen



General Settings

HDMI Input

- Set **HDMI Input** to **Enable** to allow the AM-200/AM-300 to receive a signal from a device connected to the HDMI input.
- Set **HDMI Input** to **Disable** to prevent the AM-200/AM-300 from receiving a signal from a device connected to the HDMI input.

HDCP Support

- Set **HDCP Support** to **Enable** to allow source signals that require HDCP compliance to pass through to the display device that is connected to the HDMI output.
- Set **HDCP Support** to **Disable** to prevent source signals that require HDCP compliance from passing through to the display device that is connected to the HDMI output.

NOTE: When **HDCP Support** is set to **Enable**, the display device must be HDCP compliant as well.

EDID

EDID is a data structure provided by a digital display device to describe its capabilities to a video source (i.e., graphics card or set-top box). It is what enables a modern personal computer to know what kinds of monitors are connected to it.

The EDID section of the HDMI INPUT screen specifies the EDID profile that is selected for use. Only source devices that use the selected EDID profile are allowed to send signals through the device.

Use an EDID Profile

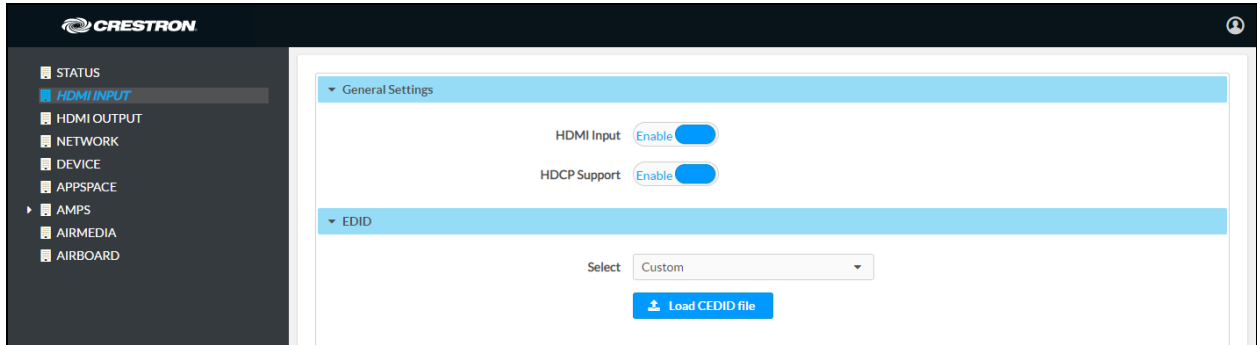
To select an EDID profile to support, select one of the profiles from the drop-down list, and click **Apply CEDID**.

Load a Custom EDID Profile

If a profile is not shown on the drop-down list, a custom profile can be loaded onto the device.

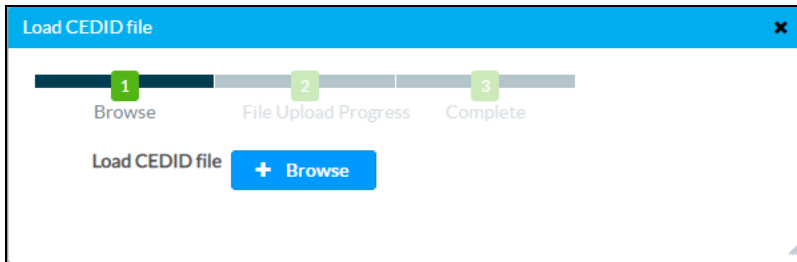
1. From the **Select** drop-down list, select **Custom**.

HDMI Input Screen



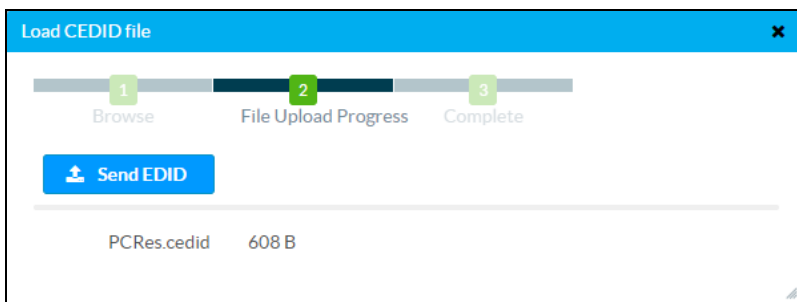
2. Click **Load CEDID file**. The Load CEDID dialog box is displayed.

Load CEDID Dialog Box



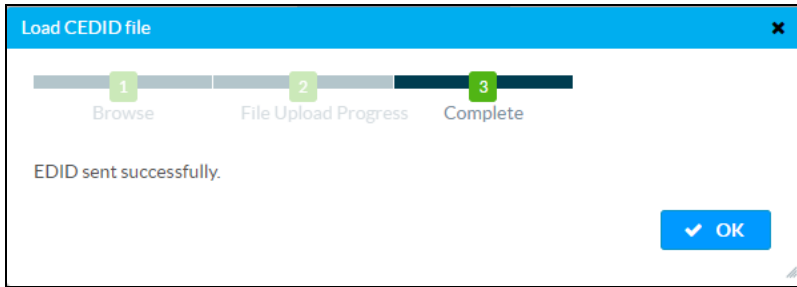
3. Click **Browse** and navigate to the location of the custom CEDID file.
4. Select the file to use and click **Open**.

Load CEDID Dialog Box



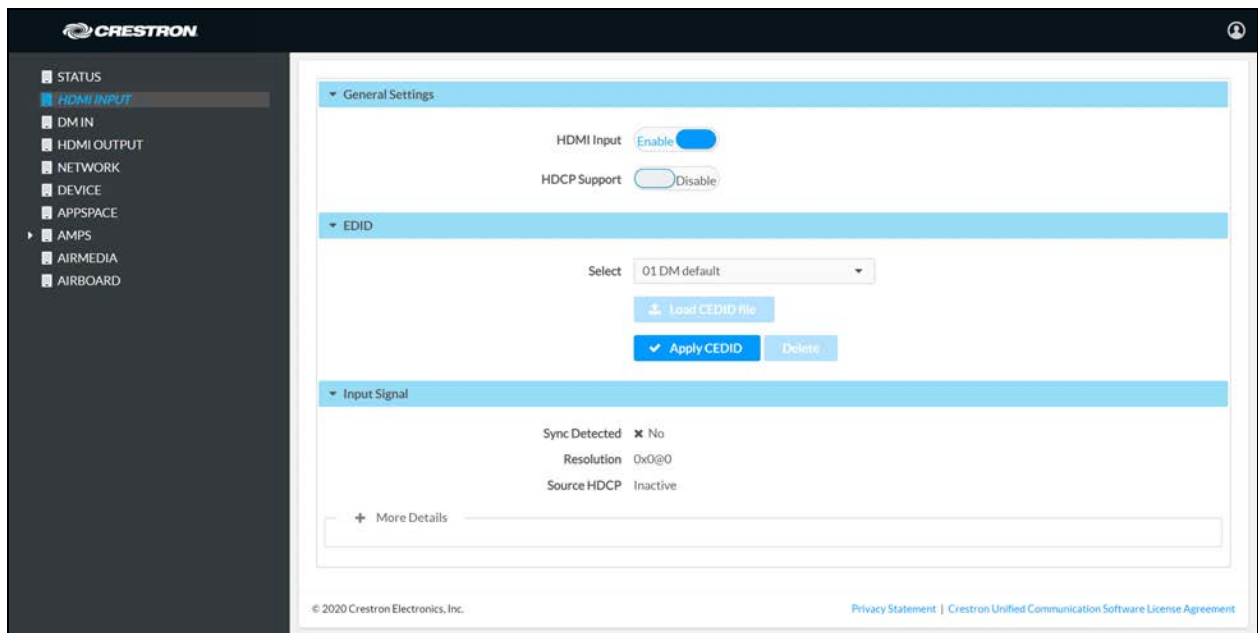
5. Click **Send EDID**. A success message is displayed.

Load CEDID Dialog Box



6. Click **OK**. The dialog box will close.

HDMI INPUT Screen



7. Select the new EDID profile from the **Select** drop-down list, and click **Apply CEDID**.

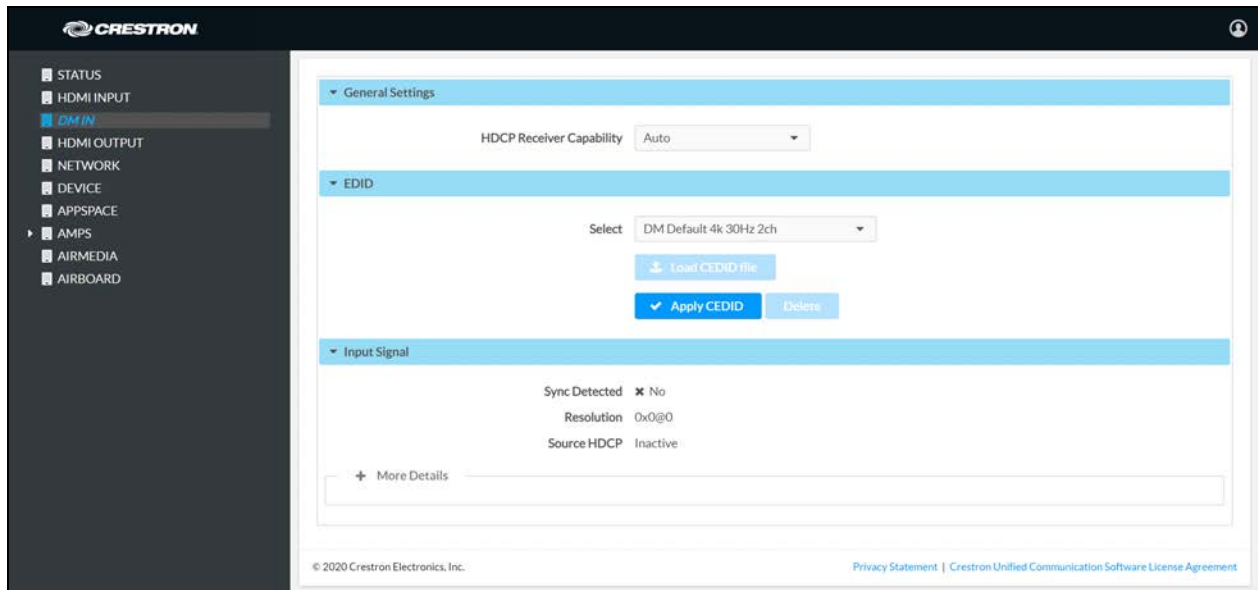
Input Signal

Click **Input Signal** to view details about the input signal connected to the HDMI input port.

DM IN (AM-300 Only)

Click **DM IN** to configure the DM input. The screen displays controls for HDCP Receiver Capability and EDID, as well as information about the input signal (if present).

DM IN Screen



General Settings

HDCP Receiver Capability

Select the desired HDCP functionality from the **HDCP Receiver Capability** drop-down list.

- **Disabled** disables the receiving of HDCP signals.
- **Auto** automatically detects the type of HDCP being received and sets it accordingly.
- **HDCP 1.4** sets the signal type to HDCP 1.4.
- **HDCP 2.2** sets the signal type to HDCP 2.2.

EDID

EDID is a data structure provided by a digital display device to describe its capabilities to a video source (i.e., graphics card or set-top box). It is what enables a modern personal computer to know what kinds of monitors are connected to it.

The EDID section of the DM IN screen specifies the EDID profile that is selected for use. Only source devices that use the selected EDID profile are allowed to send signals through the device.

Use an EDID Profile

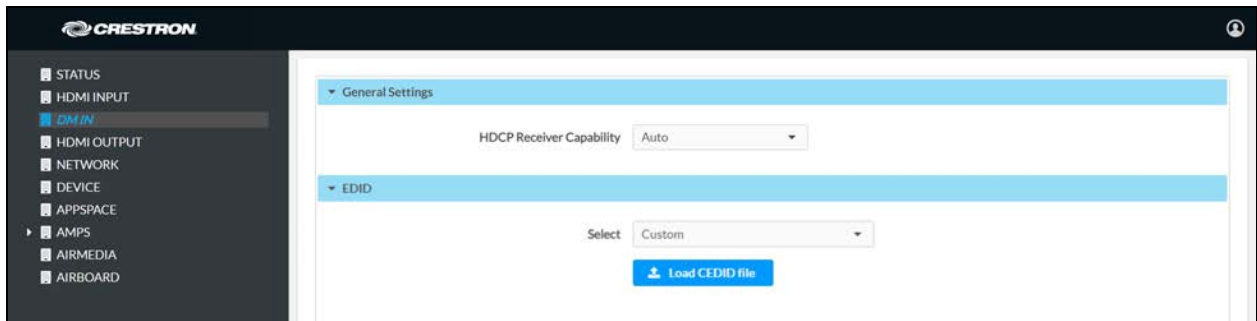
To select an EDID profile to support, select one of the profiles from the drop-down list, and click **Apply CEDID**.

Load a Custom EDID Profile

If a profile is not shown on the list, a custom profile can be loaded onto the device.

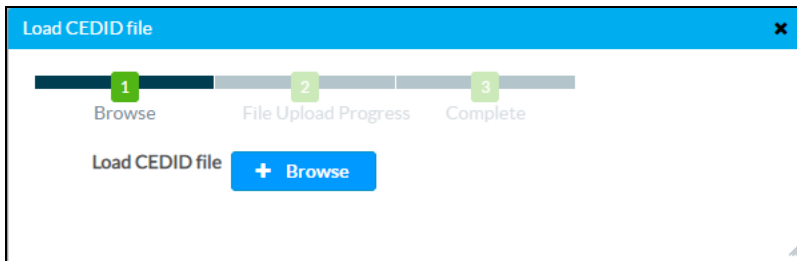
1. From the **Select** drop-down list, select **Custom**.

DM Input Screen



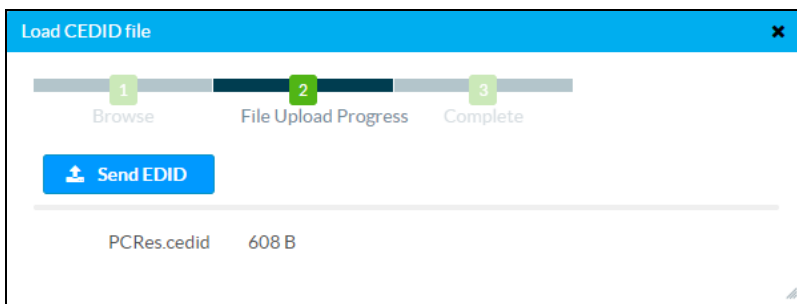
2. Click **Load CEDID file**. The Load CEDID dialog box is displayed.

Load CEDID Dialog Box



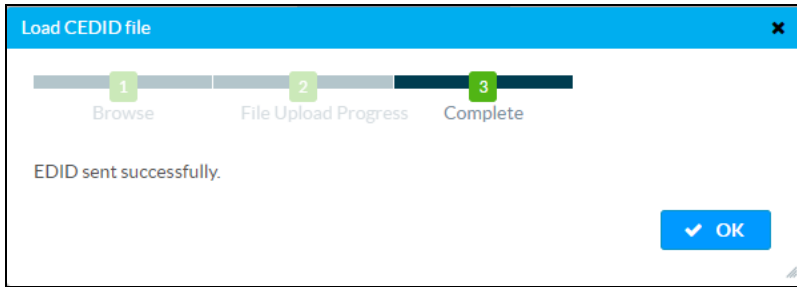
3. Click **Browse** and navigate to the location of the custom CEDID file.
4. Select the file to use and click **Open**.

Load CEDID Dialog Box



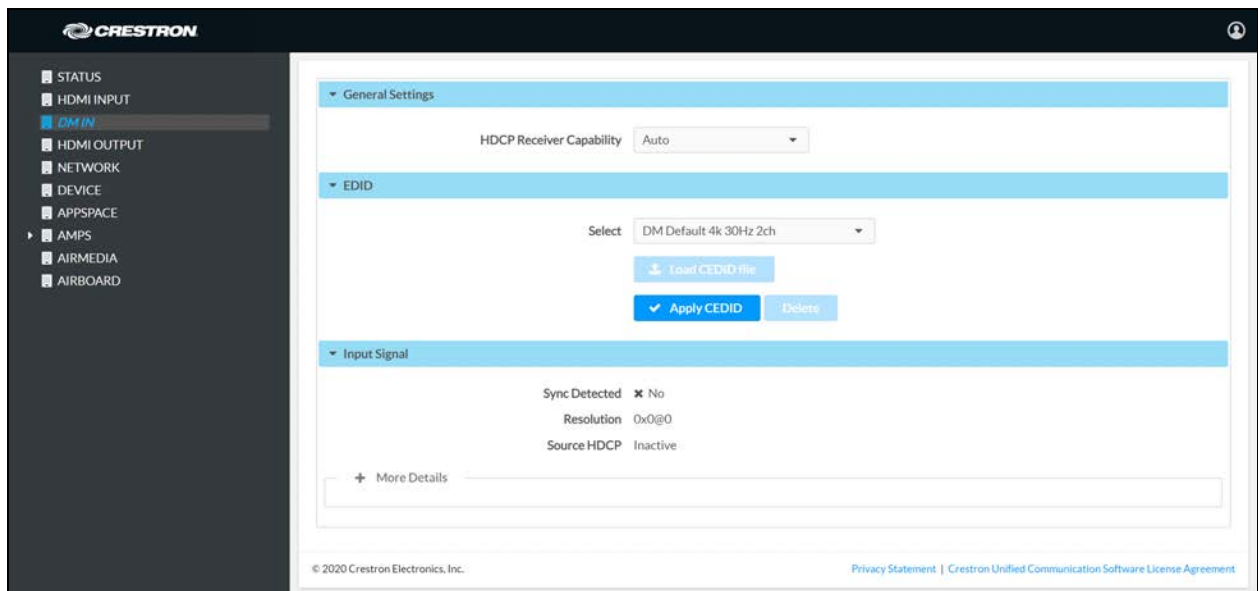
5. Click **Send EDID**. A success message is displayed.

Load CEDID Dialog Box



6. Click **OK**. The dialog box will close.

DM INPUT Screen



7. Select the new EDID from the **Select** drop-down list, and click **Apply CEDID**.

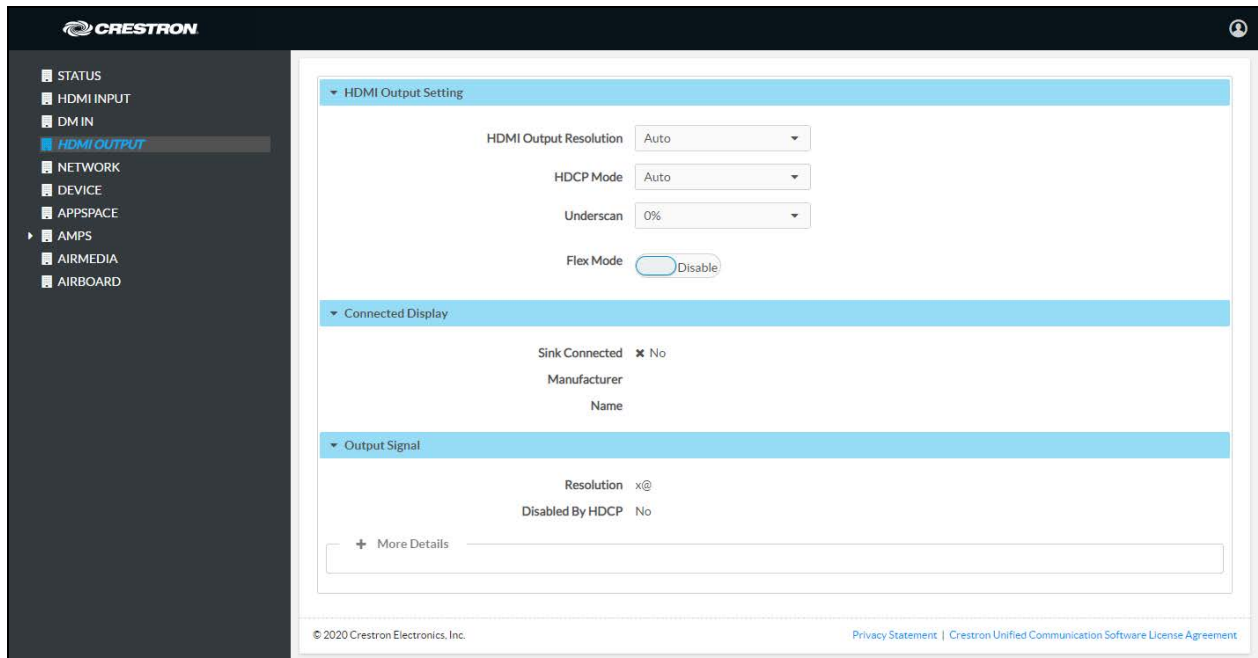
Input Signal

Click **Input Signal** to view details about the input signal connected to the DM input port.

HDMI OUTPUT

Click **HDMI OUTPUT** to change settings for the HDMI OUTPUT port and to display information about the display device and output signal.

HDMI OUTPUT Screen



HDMI Output Setting

- Select the output resolution from the **HDMI Output Resolution** drop-down list.
- Select the HDCP mode from the **HDCP Mode** drop-down list.
 - When **HDCP Mode** is set to **Auto**, the device will always attempt to use HDCP compliance if support is detected on the display device.
 - When **HDCP Mode** is set to **Always** (AM-300 only), the device will always attempt to use HDCP compliance even if downstream devices do not support HDCP.
 - When **HDCP Mode** is set to **Never**, the device will never attempt to use HDCP compliance with downstream devices, regardless of support.
- Select the amount of underscan to apply to the output signal from the **Underscan** drop-down list.
 - Apply underscan to ensure the readability of text information that may be cropped by the display device due to overscan or underscan conditions.

- When the AM-200/AM-300 is used in conjunction with a Crestron Flex kit, Flex Mode may be used to disable HDMI video output unless a source is currently active. To turn Flex Mode on, set **Flex Mode** to **Enable**. To turn Flex Mode off, set **Flex Mode** to **Disable**.

NOTE: When using the AM-200/AM-300 in Flex Mode, it is recommended that HDCP Mode is set to **Never**. Additionally, the touch screen must be set to communicate to the AM-200/AM-300 device at IP ID "FD". While in Flex Mode, the AM-200/AM-300's Standby Mode must be set to **Always On** under **AMPS > System > Power Settings**.

Connected Display

Click **Connected Display** to view details about the display device connected to the HDMI output port.

Output Signal

Click **Output Signal** to view details about the signal sent to the HDMI output port.

NETWORK

Click **NETWORK** to configure the device for operating in a network environment. There are controls for configuring the network settings, network proxy settings, 802.1x authentication, and wireless operation.

NOTE: Wireless operation requires use of the [AM-USB-WIFI](#) or [AM-USB-WF](#) AirMedia® USB Adapter with Wi-Fi® Connectivity (sold separately).

Network Setting

Configure the network settings.

NETWORK Screen – Network Setting

The screenshot displays the Crestron Network Setting interface. On the left is a dark sidebar menu with the following items: STATUS, HDMI INPUT, DM IN, HDMI OUTPUT, NETWORK (highlighted in blue), DEVICE, APPSPACE, AMPS, AIRMEDIA, and AIRBOARD. The main panel is titled 'Network Setting' and features a 'Revert' button and a 'Save Changes' button in the top right. The configuration fields are as follows:

- Host Name: AM-300-00107F9BB
- Domain Name: crestron.com
- SSH: Enabled (toggle switch)
- Primary Static DNS: [Empty field]
- Secondary Static DNS: [Empty field]

The 'Adapter' section is expanded, showing:

- DHCP: Enabled (toggle switch)
- IP Address: 10.254.44.5
- Subnet Mask: 255.255.252.0
- Default Gateway: 10.254.44.10

Below the Adapter section are three expandable sections:

- Network Proxy Settings (with Revert and Save Changes buttons)
- 802.1x Configuration (with Revert and Save Changes buttons)
- Wireless Configuration

The footer contains the text: © 2020 Crestron Electronics, Inc. and links for Privacy Statement and Crestron Unified Communication Software License Agreement.

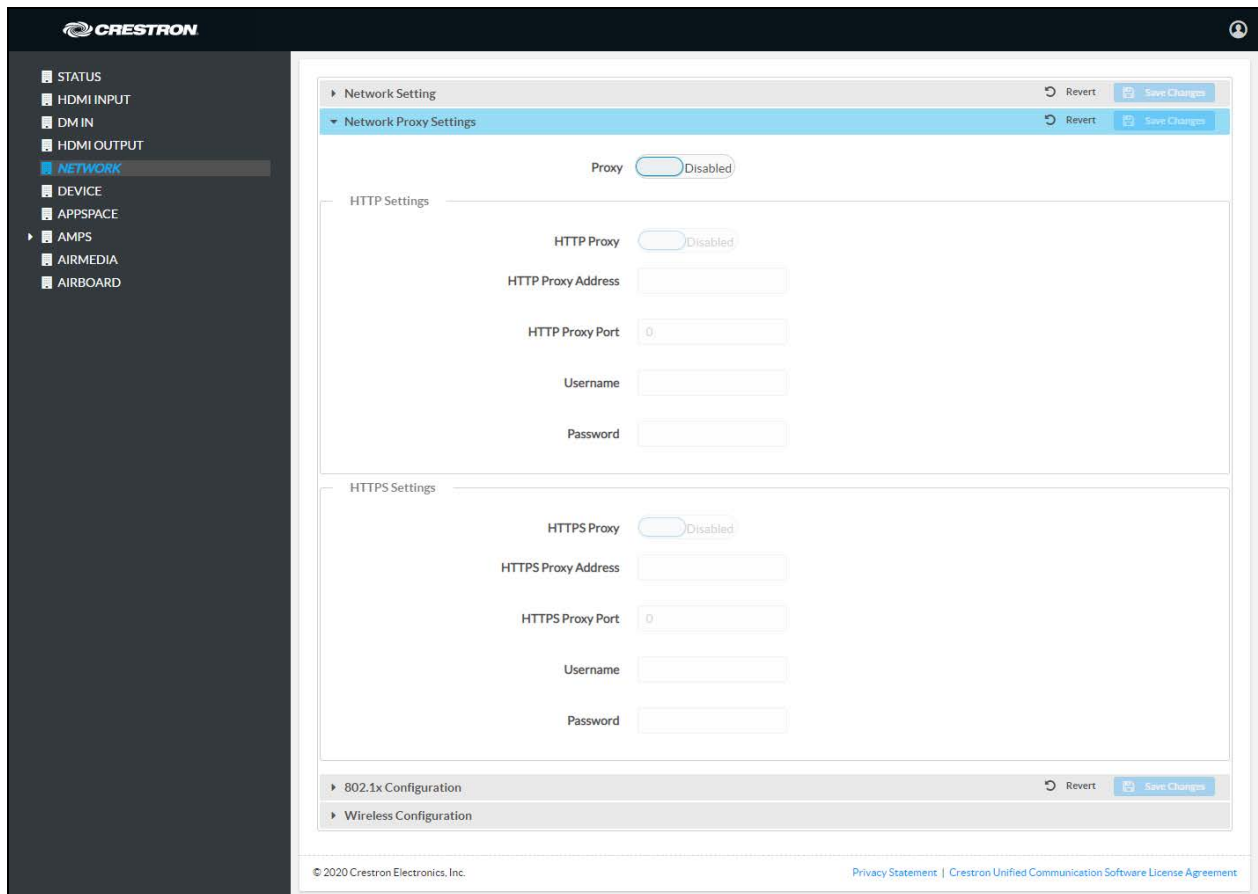
1. Enter a host name (22 characters or less) in the **Host Name** field and a domain name (optional) in the **Domain Name** field.

NOTE: Use a host name and domain name as an alternative to IP addressing for connecting client computers to the device.

2. Set Secure Shell protocol (**SSH**) to **Enabled** or **Disabled**.
3. The AM-200/AM-300 can use a DHCP server to provide the IP address, subnet mask, default gateway, and DNS settings or the Ethernet parameters can be entered manually. Choose one of the following options in the **Adapter 1** section.
 - Set **DHCP** to **Enabled** to use a DHCP server to provide the IP address, subnet mask, default gateway, and DNS server.
 - Set **DHCP** to **Disabled** to manually enter the IP address, subnet mask, default gateway, and DNS server.
4. Click **Save Changes** to apply any changes or click **Revert** to revert back to the previously used settings.

Network Proxy Settings

NETWORK Screen – Network Proxy Settings



Set **Proxy** to **Enabled** to configure the AM-200/AM-300 for use with a proxy server. To prevent the AM-200/AM-300 from using any proxy server, set **Proxy** to **Disabled**.

Configure the following settings to use the AM-200/AM-300 with an HTTP or HTTPS proxy server. When complete, click **Save Changes** to apply any changes or click **Revert** to revert back to the previously used settings.

HTTP Settings

- **HTTP Proxy:** Set **HTTP Proxy** to **Enabled** to allow the AM-200/AM-300 to use an HTTP proxy server. Set **HTTP Proxy** to **Disabled** to prevent the AM-200/AM-300 from using an HTTP proxy server.
- **HTTP Proxy Address:** Enter the IP address 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.

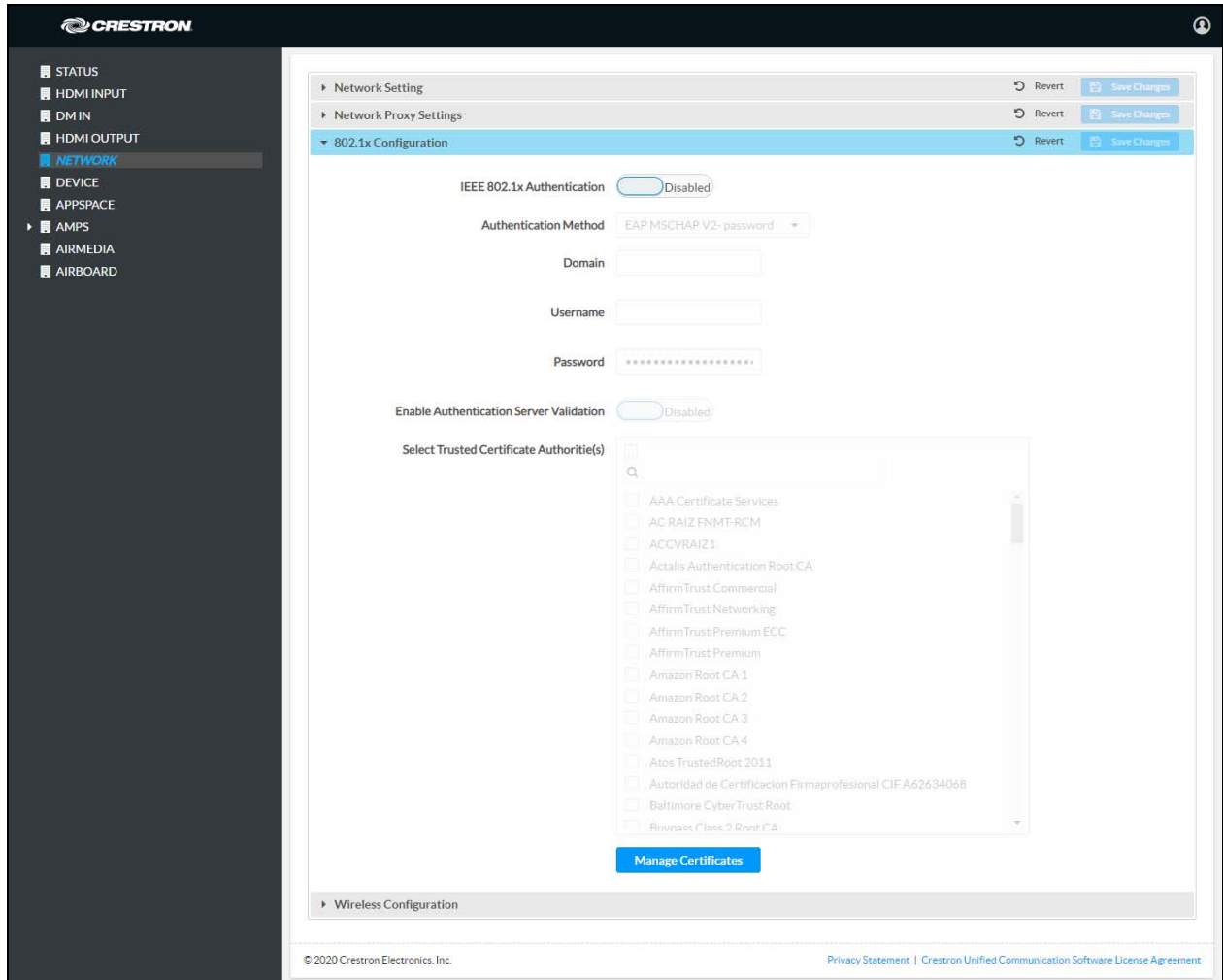
HTTPS Settings

- **HTTPS Proxy:** Set **HTTPS Proxy** to **Enabled** to allow the AM-200/AM-300 to use an HTTPS proxy server. Set **HTTPS Proxy** to **Disabled** to prevent the AM-200/AM-300 from using an HTTPS proxy server.
- **HTTPS Proxy Address:** Enter the IP address 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.

802.1x Configuration

Some networks require devices to use 802.1x port-based network access control for access to the network.

NETWORK Screen – 802.1x Configuration



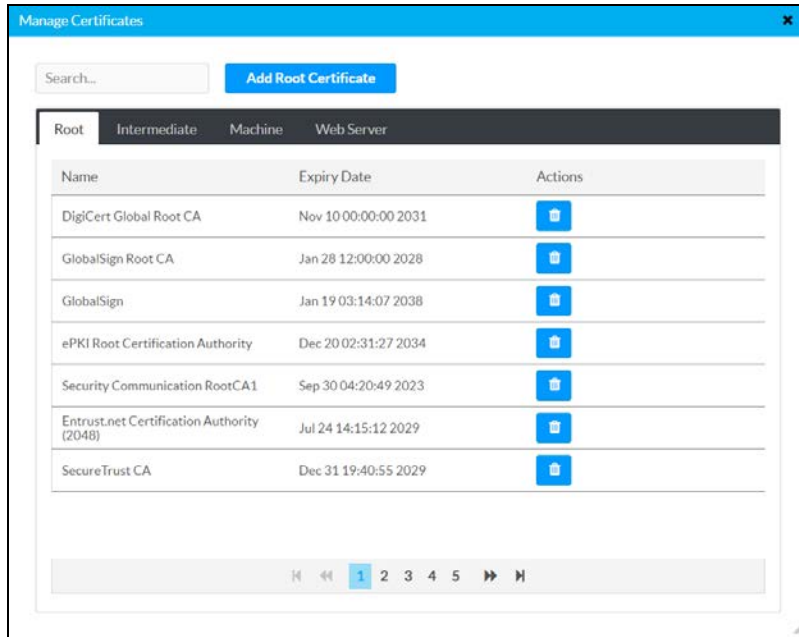
To use 802.1x, set **IEEE 802.1x Authentication** to **Enabled** and select the desired method of authentication.

Certificate Authentication

1. Select **EAP-TLS Certificate** from the **Authentication Method** drop-down list.
2. Upload a machine certificate.

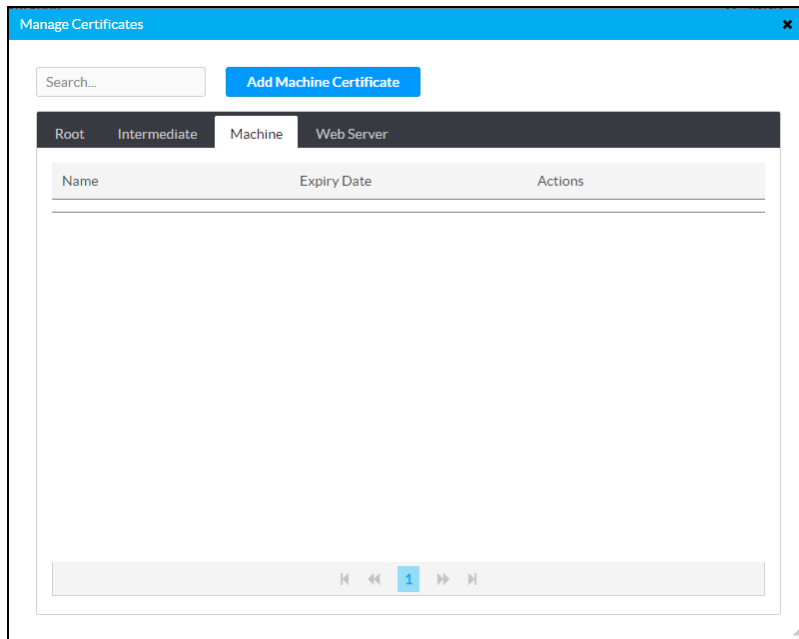
- a. Click **Manage Certificates**. A list of certificates is displayed.

Manage Certificates Dialog Box



- b. Click the **Machine** tab. Loaded certificates are displayed.

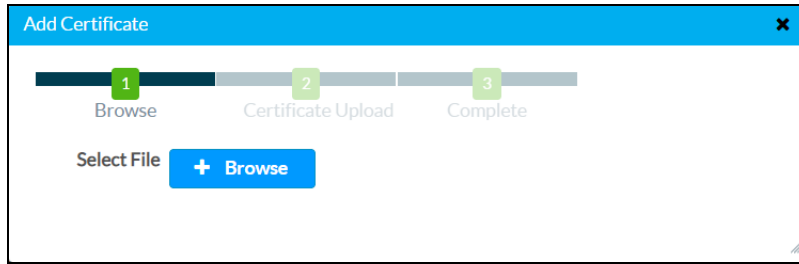
Manage Certificates Dialog Box



- c. Click to delete the certificate from the list of certificates.

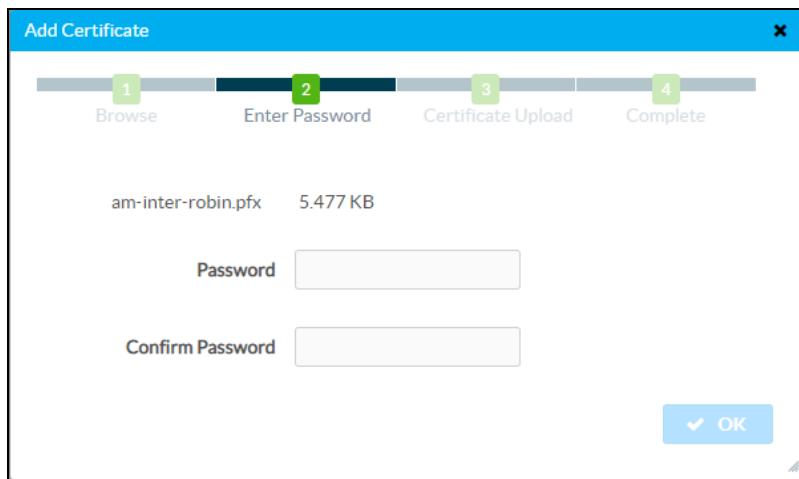
- d. Click **Add Machine Certificate**. The Add Certificate dialog box is displayed.

Add Certificate Dialog Box – Browse



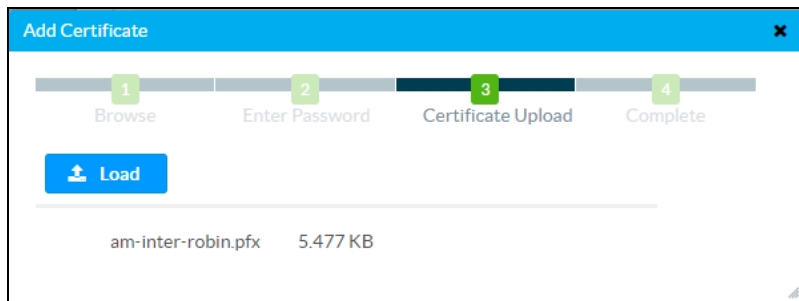
- e. Click **Browse**, select the certificate file, and click **Open**.

Add Certificate Dialog Box – Enter Password



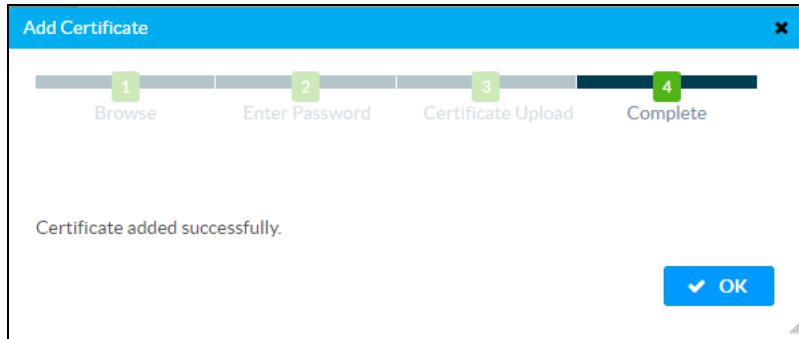
- f. Enter the password used to encrypt the file in the **Password** and **Confirm Password** fields and click **OK**.

Add Certificate Dialog Box – Load



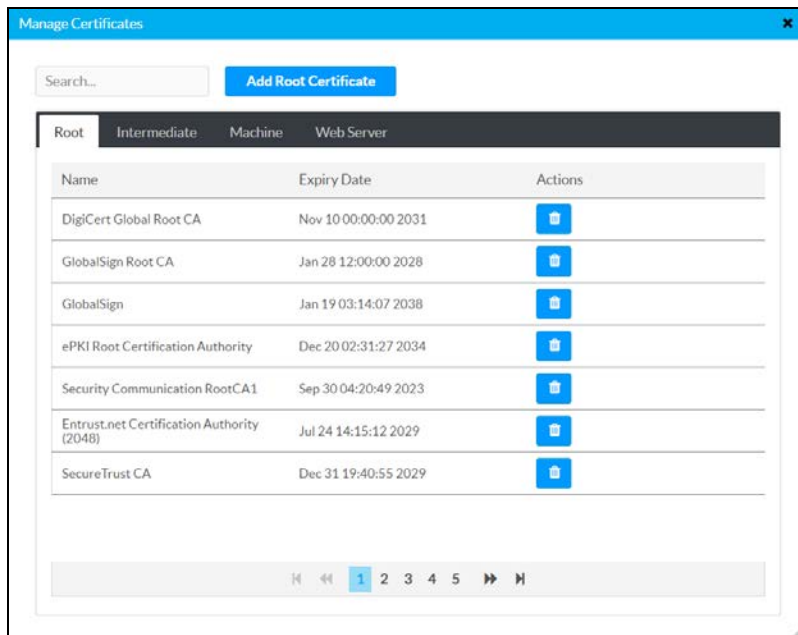
- g. Click **Load** to upload the certificate to the device. A message confirming the upload is displayed.

Add Certificate Dialog Box – Certificate Added Successfully



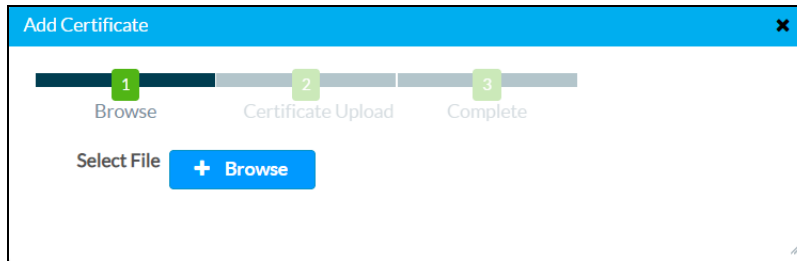
- h. Click **OK** to close the **Add Certificate** dialog box.
3. If authentication server validation is not used, set **Enable Authentication Server Validation** to **Disabled** and continue to step 5. Otherwise, set **Enable Server Validation** to **Enabled** and select the trusted certificate authorities to use.
 - To select all of the authorities, click the check box next to the search box. To unselect all of the authorities, click the check box again.
 - To search for a specific authority, start typing the name of the authority in the search box and check the box next to the desired authority.
 4. Click **Manage Certificates** to manage certificates for 802.1x authentication. A list of certificates is displayed.

Manage Certificates Dialog Box



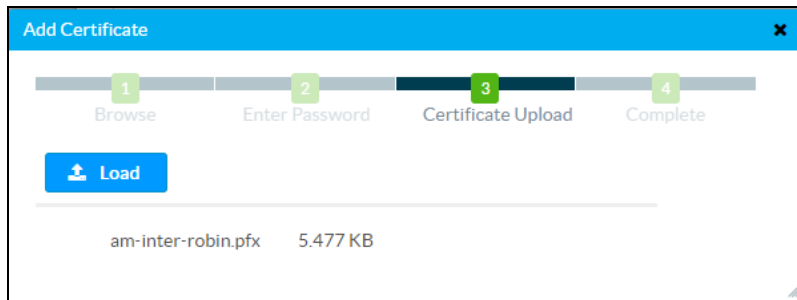
- a. Click  to delete a certificate from the list of certificates.
- b. Click **Add Root Certificate**. The **Add Certificate** dialog box is displayed.

Add Certificate Dialog Box – Browse



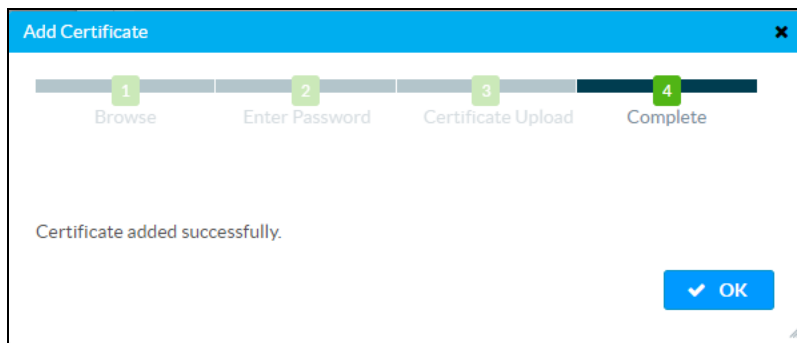
- c. Click **Browse**, select the certificate file, and click **Open**.

Add Certificate Dialog Box – Load



- d. Click **Load** to upload the certificate to the device. A message confirming the upload is displayed.

Add Certificate Dialog Box – Certificate Added Successfully

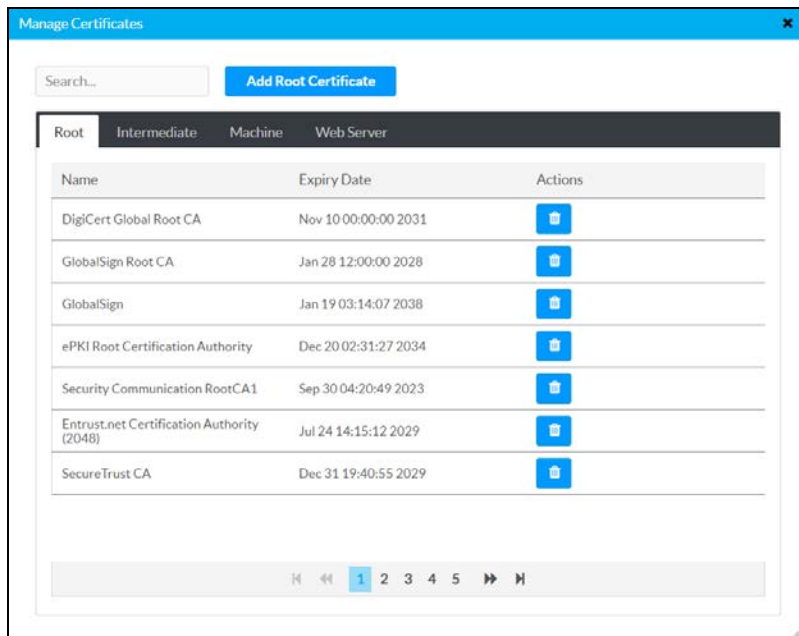


- e. Click **OK** to close the **Add Certificate** dialog box.
5. Click **Save Changes** to apply any changes or click **Revert** to revert back to the previously used settings.

Password Authentication

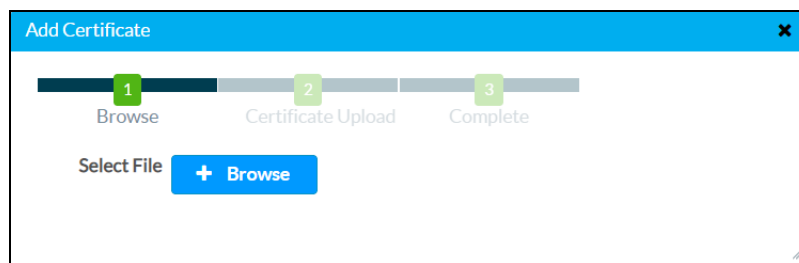
1. Select **EAP-MSCHAP V2-password** from the **Authentication Method** drop-down list .
2. Enter the domain name of the authentication server, the user name, and the password in their respective fields.
3. Set **Enable Authentication Server Validation** to **Enabled** and select the trusted certificate authorities to use.
 - To select all of the authorities, click the check box next to the search box. To unselect all of the authorities, click the check box again.
 - To search for a specific authority, start typing the name of the authority in the search box and check the boxes next to the desired authorities.
4. Click **Manage Certificates** to load a custom certificate, A list of certificates is displayed.

Manage Certificates Dialog Box



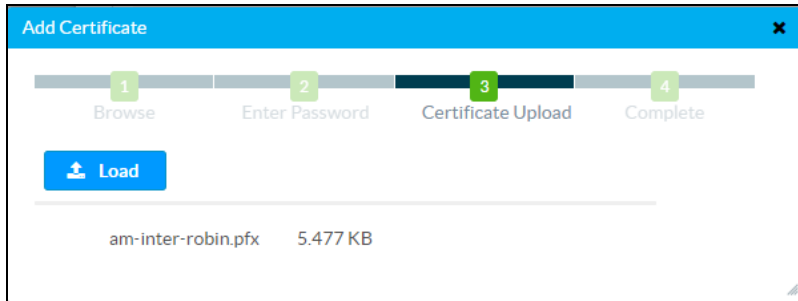
- a. Click to delete a certificate from the list of certificates.
- b. Click **Add Root Certificate**. The **Add Certificate** dialog box is displayed.

Add Certificate Dialog Box – Browse



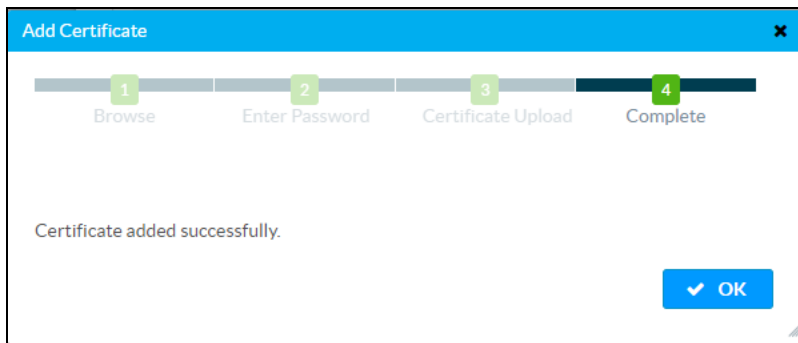
- c. Click **Browse**, select the certificate file, and click **Open**.

Add Certificate Dialog Box – Load



- d. Click **Load** to upload the certificate to the device. A message confirming the upload is displayed.

Add Certificate Dialog Box – Certificate Added Successfully



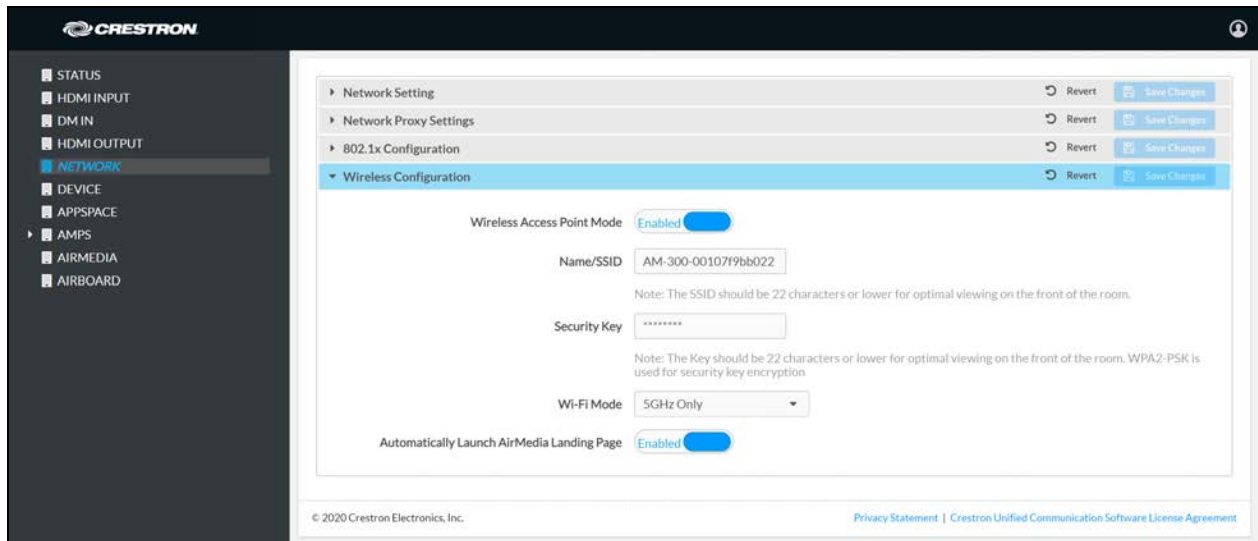
- e. Click **OK** to close the **Add Certificate** dialog box.
5. Click **Save Changes** to apply any changes or click **Revert** to revert back to the previously used settings.

Wireless Configuration

When equipped with the [AM-USB-WIFI](#) or [AM-USB-WF](#) AirMedia USB Adapter with Wi-Fi Connectivity (sold separately), the AM-200/AM-300 can be used as a Wireless Access Point (WAP) so users can present wirelessly without using a corporate Wi-Fi network.

NOTE: Use of the AM-USB-WIFI or AM-USB-WF-I prevents use of the [ZUMMESH-AVBRIDGE](#), [ZUMMESH-AVBRIDGE-I](#), [ZUMMESH-KP10AMBATT](#), and [ZUMMESH-PIR-OCCUPANCY-BATT](#).

NETWORK Screen – Wireless Configuration



1. Set **Wireless Access Point Mode** to **Enabled** to use the AM-200/AM-300 as a wireless access point. Set **Wireless Access Point Mode** to **Disabled** to disable the feature.
2. Enter a name for the wireless network in the **Name/SSID** field.

NOTE: For optimal viewing on the display device and a connected touch screen, the name should be 22 characters or less.

3. Enter a security key in the **Security Key** field.

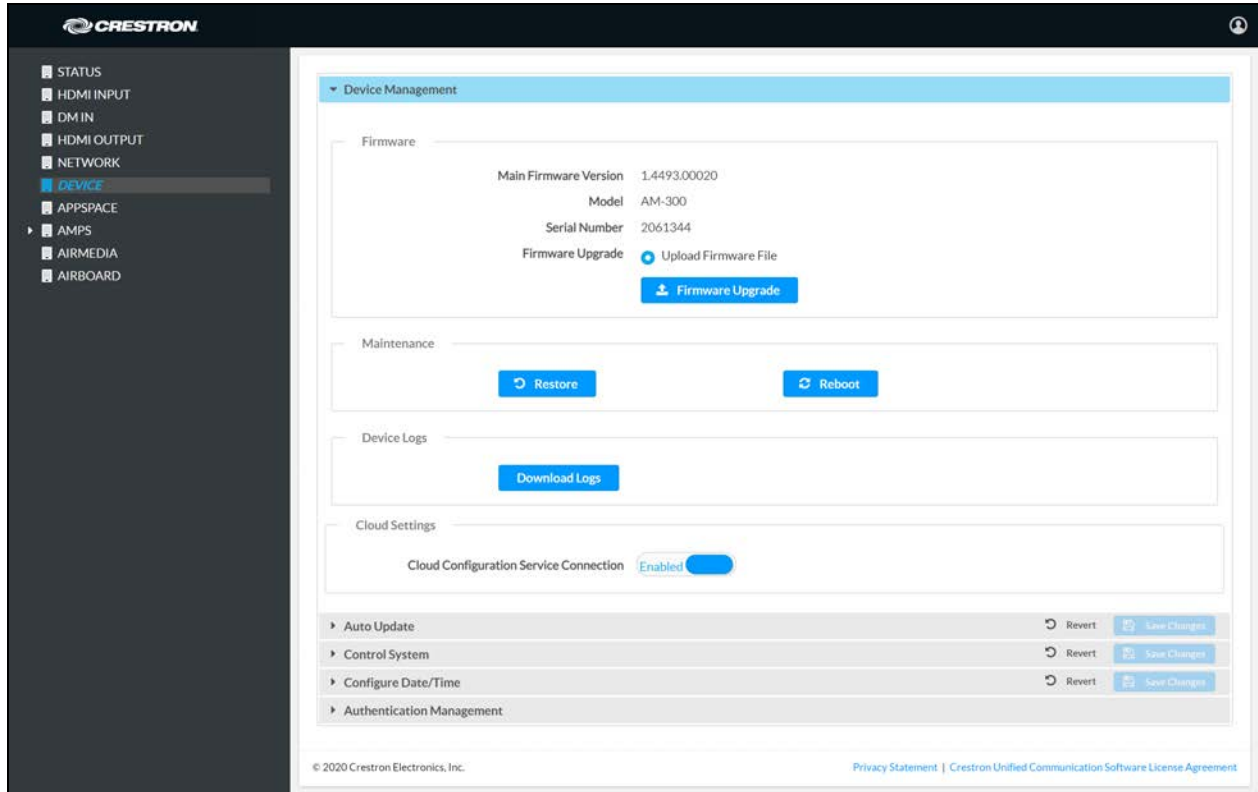
NOTES:

- WPA2-PSK is used for security key encryption.
 - For optimal viewing on the display device and a connected touch screen, the security key should be 22 characters or less.
4. Select the Wi-Fi mode from the **Wi-Fi Mode** drop-down list.
 - Select **2.4GHz Only** to use the 2.4 GHz frequency band.
 - Select **5GHz Only** to use the 5 GHz frequency band.
 5. Select whether the AM-200/AM-300 should automatically launch a web browser and redirect the user to the AirMedia landing page upon connection to the wireless access point.
 - Select **Enabled** to automatically launch a web browser and redirect the user to the AirMedia landing page upon connection to the wireless access point.
 - Select **Disabled** to disable the feature.
 6. Click **Save Changes** to apply any changes or click **Revert** to revert back to the previously used settings.

DEVICE

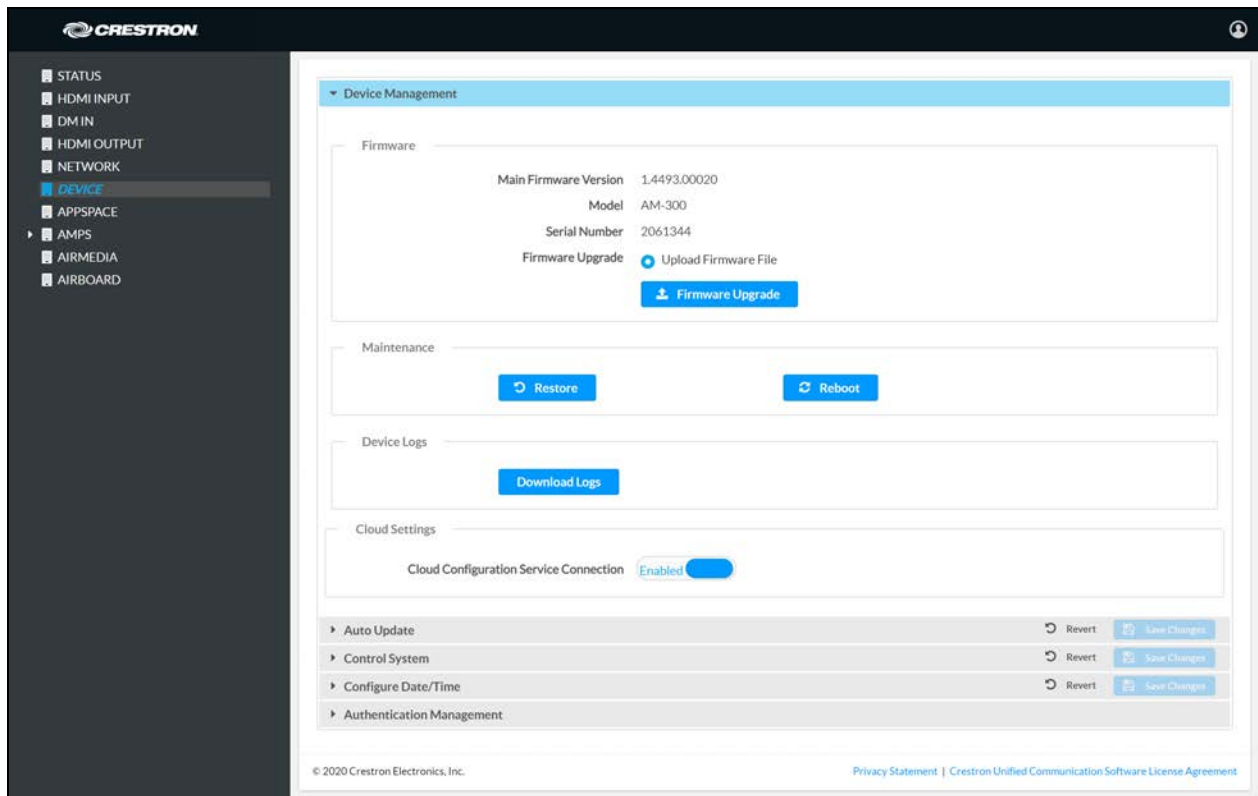
Click **DEVICE** to manage the device, enable automatic updates, identify the device to a control system, configure date and time, and configure authentication management.

DEVICE Screen



Device Management

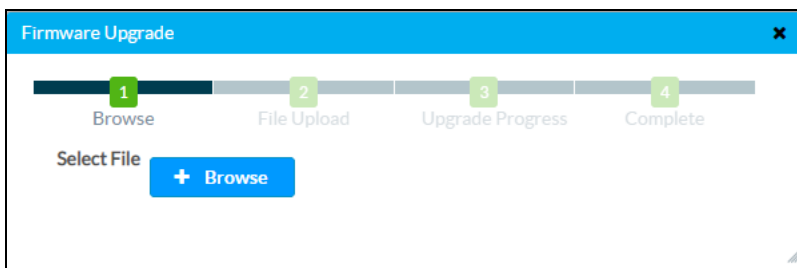
DEVICE Screen – Device Management



Upgrade Firmware

1. Click **Firmware Upgrade**.

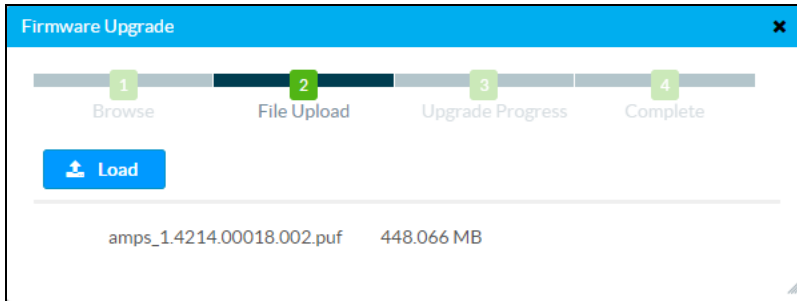
Firmware Upgrade Dialog Box – Browse



2. Click **Browse** and navigate to the location of the firmware file.

3. Select the file to use and click **Open**.

Firmware Upgrade Dialog Box – Load



4. Click **Load** to load the firmware.

Maintenance

Click **Restore** to restore the factory settings. Click **Reboot** to reboot the device.

NOTE: If the device is restored to factory settings, the default user name and password used to configure the AM-200/AM-300 will be restored as well. Any custom user names or passwords will no longer work.

Device Logs

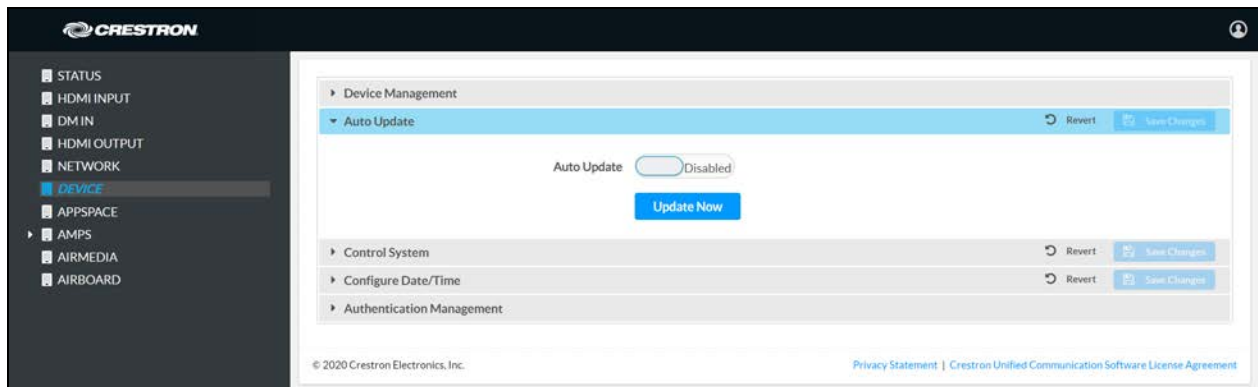
Click **Download Logs** to download the device's system logs to the PC.

Cloud Settings

The **Cloud Settings** section controls the device's connection to the XiO Cloud® service. By default, the **Cloud Configuration Service Connection** is set to **Enabled**. To disable the connection, set **Cloud Configuration Service Connection** to **Disabled**. For more information, refer to [XiO Cloud Service \(on page 106\)](#).

Auto Update

DEVICE Screen – Auto Update

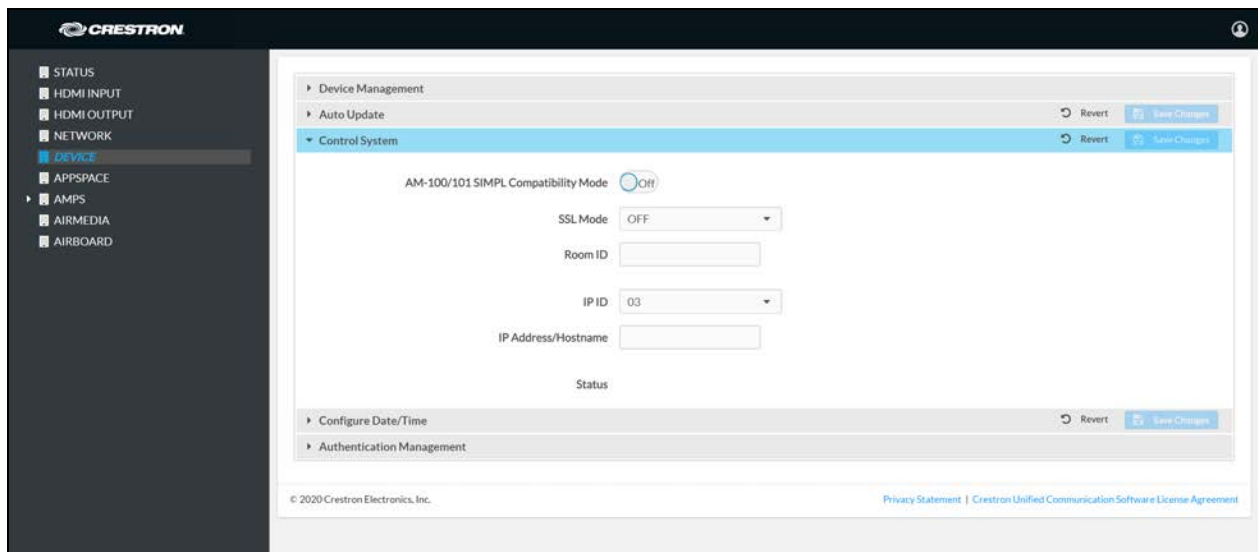


The device can automatically check for firmware updates from Crestron and update the device as needed.

- Set **Auto Update** to **Enabled** to allow automatic updates.
- Set **Auto Update** to **Disabled** to turn off automatic updates.
- Click **Update Now** to check for available updates.

Control System

DEVICE Screen – Control System (AM-200 Shown)



The device can be controlled by a Crestron control system or a virtual control system's SIMPL or SIMPL# program.

AM-100/AM-101 Compatibility (AM-200 only)

An AM-200 can be used as a direct replacement for an AM-100 or AM-101 AirMedia Presentation Gateway in a SIMPL Windows program without any reprogramming. To use the AM-200 as a replacement for an AM-100 or AM-101, set **AM-100/101 SIMPL Compatibility Mode** to **On**. Otherwise set **AM-100/101 SIMPL Compatibility Mode** to **Off**.

SSL Mode

The device can use SSL encryption for communication with the control system. SSL can be used with or without a CA certificate.

Select an SSL mode from the **SSL Mode** drop-down list.

- **OFF:** SSL is not used for communication between the device and the control system.
- **Encrypt:** SSL is used for communication between the device and the control system.
User-level authentication is optional. If you are using authentication, enter the following information.
 - **Control System Username:** The login name for the control system.
 - **Control System Password:** The password used to log in to the control system.
 - **Confirm Password:** Confirm the password used to log in to the control system.

DEVICE Screen – Control System – SSL Encrypt Mode

The screenshot displays the Crestron device management interface. On the left is a dark sidebar with a menu containing: STATUS, HDMI INPUT, HDMI OUTPUT, NETWORK, **DEVICE** (highlighted), APPSPACE, AMPS, AIRMEDIA, and AIRBOARD. The main content area is titled 'Control System' and features a toggle for 'AM-100/101 SIMPL Compatibility Mode' set to 'Off'. Below this, the 'SSL Mode' is set to 'Encrypt'. There are input fields for 'Control System Username', 'Control System Password', and 'Confirm Password'. Other fields include 'Room ID', 'IP ID' (set to '03'), and 'IP Address/Hostname'. At the bottom, there are sections for 'Configure Date/Time' and 'Authentication Management'. The footer contains the copyright notice '© 2020 Crestron Electronics, Inc.' and a link to the 'Privacy Statement | Crestron Unified Communication Software License Agreement'.

- **Encrypt and Validate:** SSL is used for communication between the device and the control system. The control system will be validated against a root CA certificate. User-level

authentication is optional. If you are using authentication, enter the following information:

- **Control System Username:** The login name for the control system.
- **Control System Password:** The password used to log in to the control system.
- **Confirm Password:** Confirm the password used to log in to the control system.

DEVICE Screen – Control System – SSL Encrypt and Validate Mode

The screenshot shows the Crestron web interface for configuring the Control System. The sidebar on the left lists various system components, with 'DEVICE' selected. The main panel is titled 'Device Management' and contains several configuration sections. The 'Control System' section is expanded, showing options for 'AM-100/101 SIMPL Compatibility Mode' (set to Off), 'SSL Mode' (set to 'Encrypt and Validate'), and input fields for 'Control System Username', 'Control System Password', and 'Confirm Password'. Below these are fields for 'Room ID', 'IP ID' (set to '03'), and 'IP Address/Hostname'. At the bottom of the main panel, there are sections for 'Configure Date/Time' and 'Authentication Management', each with 'Revert' and 'Save Changes' buttons. The footer includes the copyright notice '© 2020 Crestron Electronics, Inc.' and links to the 'Privacy Statement' and 'Crestron Unified Communication Software License Agreement'.

If you are using the **Encrypt and Validate** setting, a root certificate must be placed in the /SYS directory on the device with FTP software.

NOTE: The root certificate file name must have a *.PEM* extension. i.e. *rootCA_cert.pem*.

Control System Connection

Specify the control system connection.

1. Enter a descriptive name for the device in the **Room ID** field.
2. Select the IP ID of the device from the **IP ID** drop-down list.

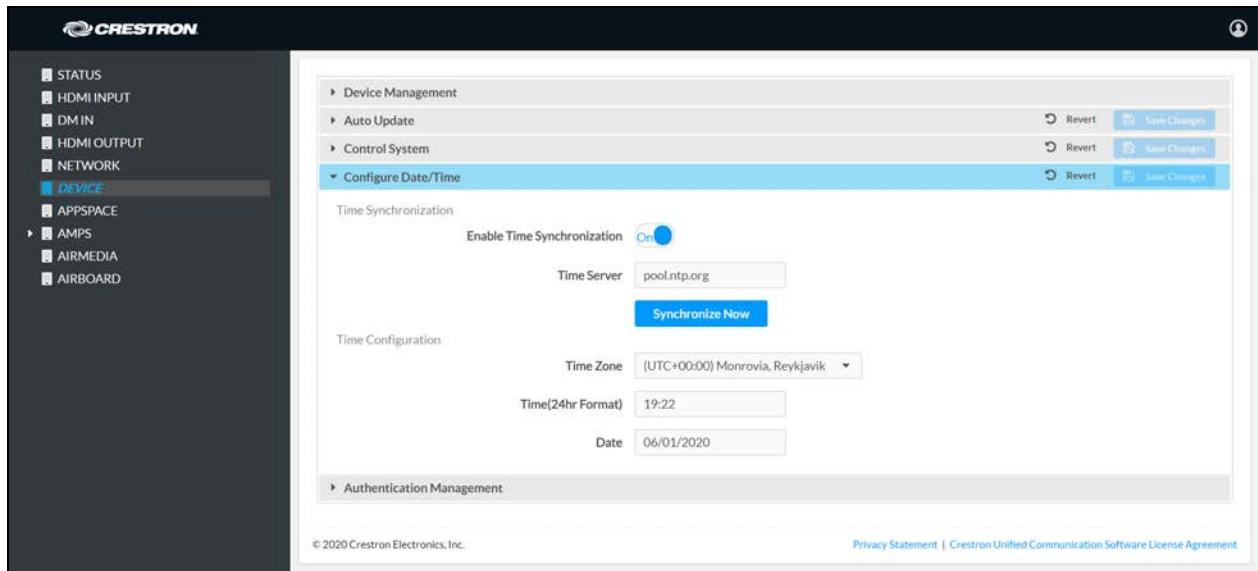
NOTE: The IP ID must match the IP ID defined in the control system's SIMPL Windows or SIMPL# program.

3. Enter the control system's IP address or host name in the **IP Address/Hostname** field.
4. Click **Save Changes** to apply any changes or click **Revert** to revert back to the previously used settings.

The **Status** field indicates a connection to the control system program if the device is listed in the control system's IP table.

Configure the Date and Time

DEVICE Screen – Configure Date/Time



The device's internal clock can be synchronized with a time server or set manually.

NOTE: The time is automatically set when connected to Crestron Fusion. Any settings made here do not apply.

Use Time Server Synchronization

1. Set **Enable Time Synchronization** to **On**.
2. Enter the time server's IP address or host name in the **Time Server** field.
3. Click **Synchronize Now** to sync the device with the specified time server.
4. Click **Save Changes** to apply any changes or click **Revert** to revert back to the previously used settings.

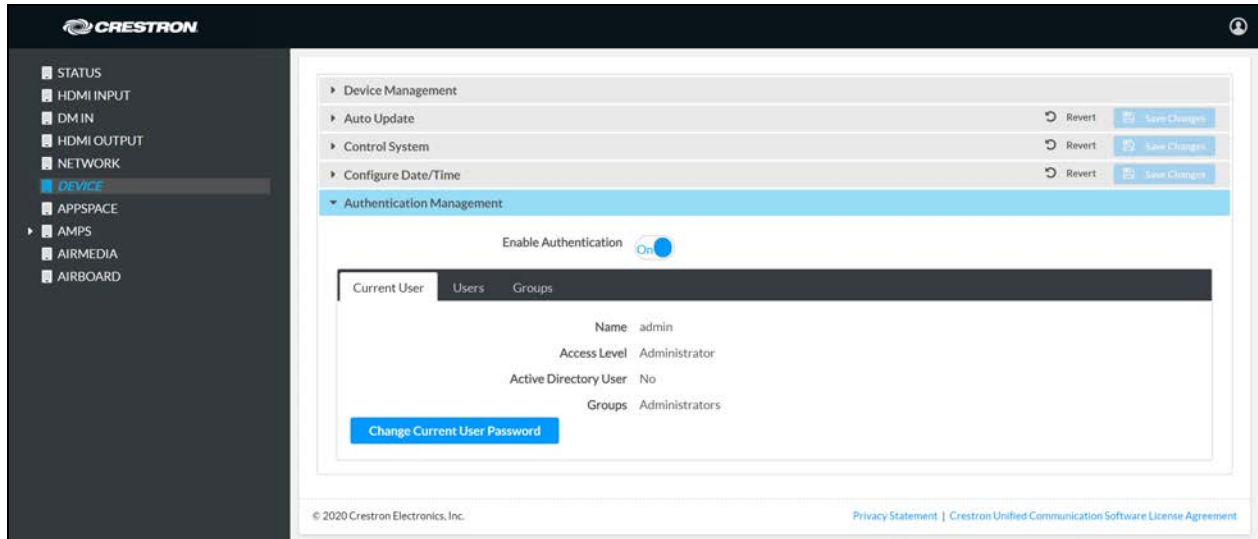
Set the Time Manually

1. Set **Enable Time Synchronization** to **Off**.
2. Select the time zone from the **Time Zone** drop-down list.
3. Enter the time (in 24 hour format) in the **Time(24hr Format)** field.
4. Click on the **Date** field, and then click a date from the pop-up calendar.

5. Click **Save Changes** to apply any changes or click **Revert** to revert back to the previously used settings.

Authentication Management

DEVICE Screen – Authentication Management



Use this section to set the password for the current user and to manage users and user groups. By default, **Enable Authentication** is set to **On**. If set to **Off**, authentication is not required to configure the device (not recommended).

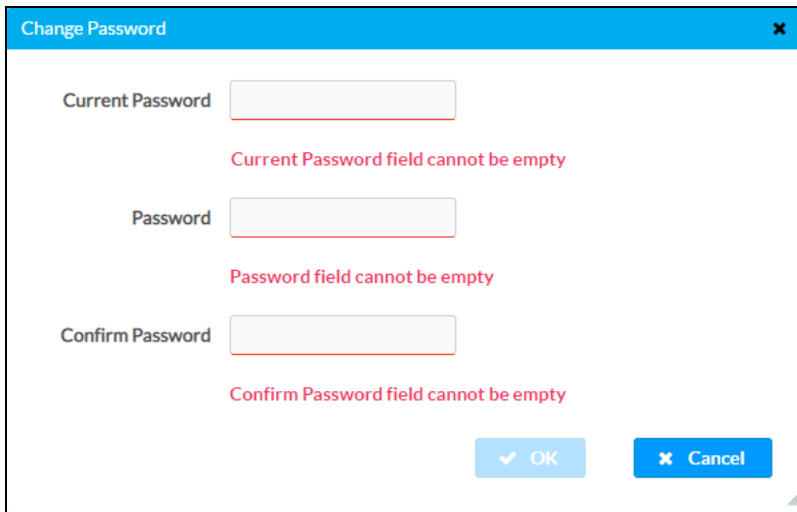
NOTE: The **Enable Authentication** setting appears in devices with firmware earlier than version 1.4492. The **Enable Authentication** setting is removed from devices that upgrade to version 1.4493 or later and are restored to factory settings. New devices with firmware version 1.4493 or later do not have the **Enable Authentication** setting.

Current User

Click the **Current User** tab to view information about the current user and change the password.

1. Click **Change Current User Password** to change the current user's password.

Change Password Dialog Box



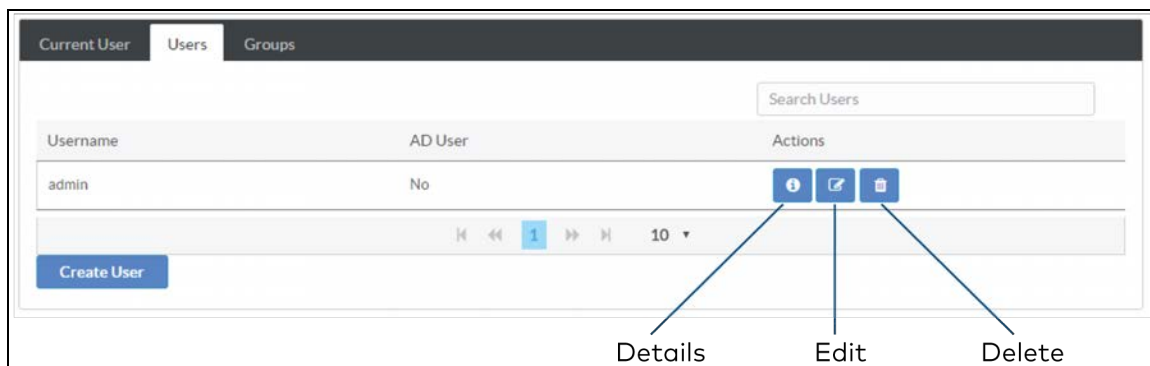
The image shows a 'Change Password' dialog box with a blue title bar and a close button. It contains three text input fields: 'Current Password', 'Password', and 'Confirm Password'. Below each field is a red error message: 'Current Password field cannot be empty', 'Password field cannot be empty', and 'Confirm Password field cannot be empty'. At the bottom right, there are two buttons: 'OK' (with a checkmark icon) and 'Cancel' (with an 'X' icon).

2. Enter the current password in the **Current Password** field.
3. Enter the new password in the **Password** field.
4. Confirm the new password in the **Confirm Password** field.
5. Click **OK** to set the new password or click **Cancel** to cancel.

Users

Click the **Users** tab to manage and create authorized users. A list of authorized users is displayed.


DEVICE Screen – Authentication Management: Users Tab




Search for a User

Enter the name in the **Search Users** field and press **Enter**.

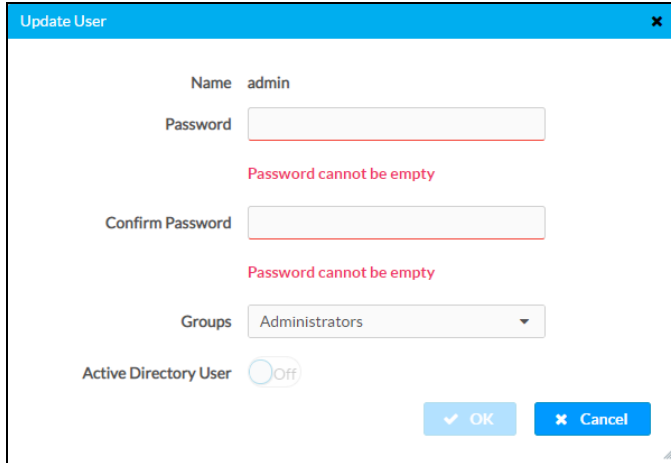
View User Details

Click  to view details about a user. Click **OK** when done.

Update a User

Click  to update a user's information.

Update User Dialog Box




The screenshot shows a dialog box titled "Update User" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Name:** A text field containing the value "admin".
- Password:** An empty text input field with a red error message "Password cannot be empty" displayed below it.
- Confirm Password:** An empty text input field with a red error message "Password cannot be empty" displayed below it.
- Groups:** A dropdown menu currently showing "Administrators".
- Active Directory User:** A radio button labeled "Off".
- Buttons:** "OK" and "Cancel" buttons are located at the bottom right of the dialog.

1. Enter the password in the **Password** field.
2. Confirm the password in the **Confirm Password** field.
3. Select the user's group memberships from the **Groups** drop-down list.
4. Set **Active Directory User** to **On** if the user is a member of the Active Directory group. Otherwise, set **Active Directory User** to **Off**.
5. Click **OK** to save the changes or click **Cancel** to cancel.

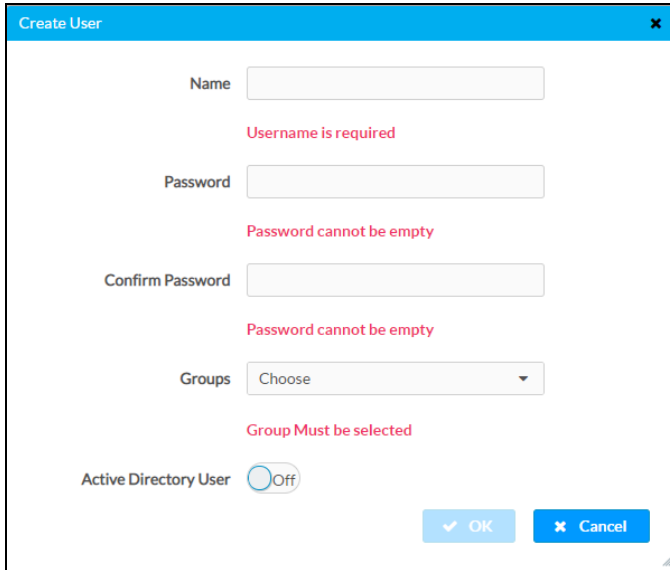
Delete a User

1. Click  to delete a user from the list of authorized users.
2. Click **Yes** to confirm or **No** to cancel.

Create a User

1. Click **Create User**. The **Create User** dialog box is displayed.

Create User Dialog Box



The screenshot shows a 'Create User' dialog box with the following fields and errors:

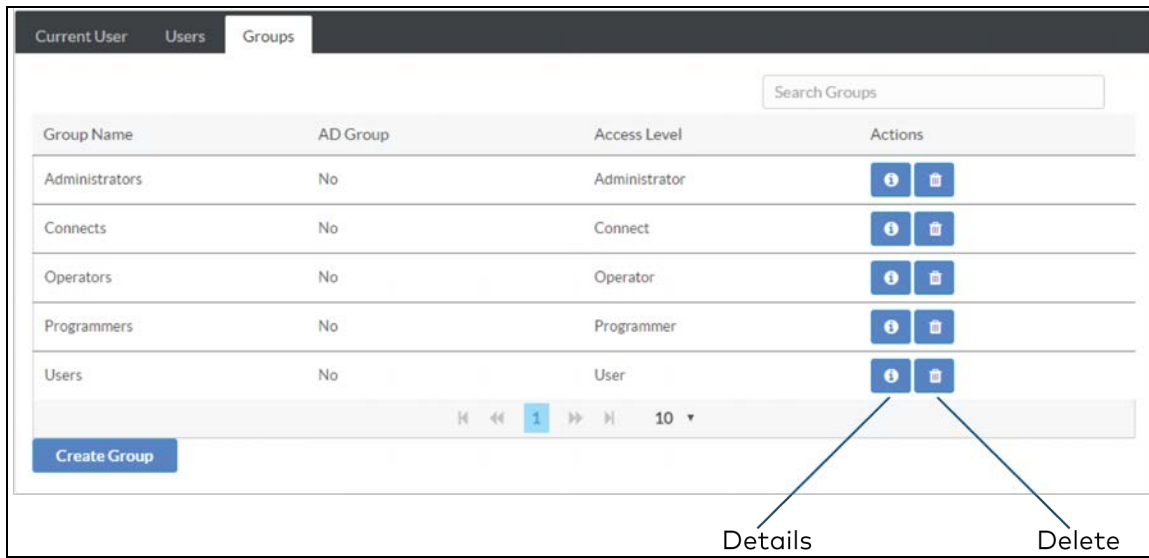
- Name**: Text input field with error message "Username is required".
- Password**: Text input field with error message "Password cannot be empty".
- Confirm Password**: Text input field with error message "Password cannot be empty".
- Groups**: Dropdown menu with "Choose" selected and error message "Group Must be selected".
- Active Directory User**: Toggle switch currently set to "Off".
- Buttons**: "OK" and "Cancel" buttons at the bottom right.

2. Enter the user name in the **Name** field.
3. Enter the user password in the **Password** field.
4. Confirm the password in the **Confirm Password** field.
5. Select the user's group memberships from the **Groups** drop-down list.
6. Set **Active Directory User** to **On** if the user is a member of the Active Directory group. Otherwise, set **Active Directory User** to **Off**.
7. Click **OK** to save the user or click **Cancel** to cancel.

User Groups

Click the **Groups** tab to configure user groups. A list of user groups is displayed.

DEVICE Screen – Authentication Management: Groups Tab



Search for a Group

Enter the name in the **Search Groups** field, and press **Enter**.

View Group Details

Click to view details about a group. Click **OK** when done.

Delete a Group

1. Click to delete a group from the list of groups.
2. Click **Yes** to confirm or **No** to cancel.

Create a User Group

1. Click **Create Group**. The **Create Group** dialog box is displayed.

Create Group Dialog Box

The 'Create Group' dialog box has a blue title bar with a close button. It contains three fields: 'Name' (text input), 'Access Level' (dropdown menu with 'Administrator' selected), and 'Active Directory Group' (radio button with 'Off' selected). At the bottom are 'OK' and 'Cancel' buttons.

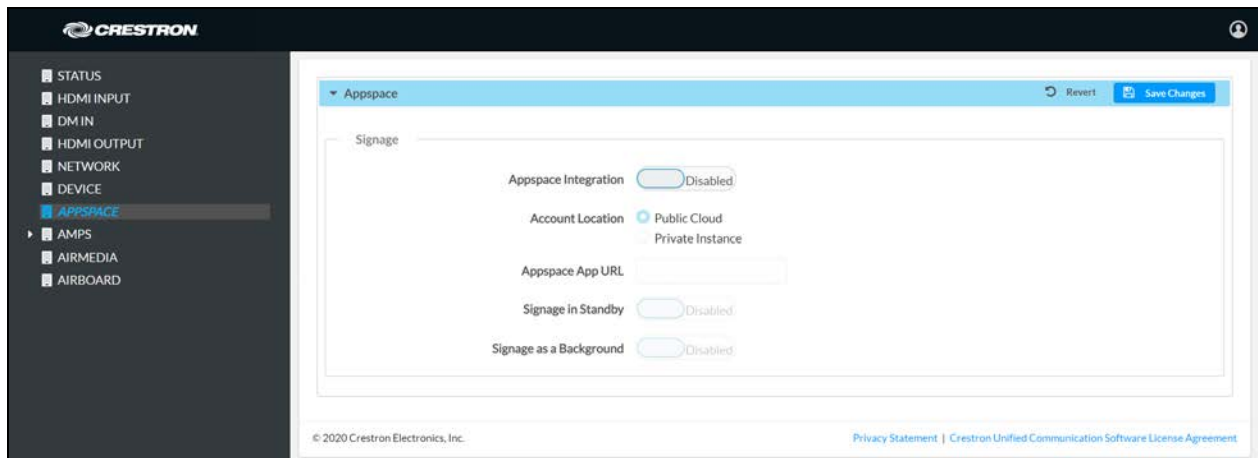
2. Enter the group name in the **Name** field.

3. Select the group's access level from the **Access Level** drop-down list.
 - **Administrator** grants full access to the system settings and device functions.
 - **Connect** grants access to the device functions.
 - **Operator** grants read access to the system settings and full access to the device functions.
 - **Programmer** grants access to program/project specific settings/ReadOnly to the rest, read/write access to the file system, no access to the setup project.
 - **User** grants access to the device functions.
4. Set **Active Directory User** to **On** if the group is a member of the Active Directory group. Otherwise, set **Active Directory User** to **Off**.
5. Click **OK** to save the group or click **Cancel** to cancel.

APPSPACE

Click **APPSPACE** to configure the device's operation with the Appspace platform. The AM-200 and AM-300 can display content from an Appspace digital signage channel when a presentation source is not active, or the room is not occupied.

APPSPACE Screen



NOTES:

- An active Appspace account is required.
- Appspace video service is not supported.

1. Set **Appspace Integration** to **Enabled** to enable Appspace when the device goes to sleep based on occupancy (Standby). When enabled, the display device will show Appspace content.

NOTE: To use Appspace when the device is in Standby, the Power Settings must be set to **Occupancy Based With Signage** as described in [Power Settings \(on page 47\)](#).

2. Choose the **Account Location**.
 - **Public Cloud:** Select this option to use the Appspace public web app.
 - **Private Instance:** Select this option to use a privately hosted instance of the Appspace web app.
3. Enter the location of the privately hosted instance of the Appspace web in the **Appspace App URL** field. Leave blank if the **Public Cloud** account location is selected.
4. Set **Signage in Standby** to **Enabled** to display Appspace content when the AM-200/AM-300 goes to sleep based on occupancy. Set to **Disabled** to turn off the feature.
5. Set **Signage as a Background** to **Enabled** to display Appspace content on the display device behind the calendar, date/time, system name, connection info, and branding portions of the display. Otherwise, set **Signage as a Background** to **Disabled**.

NOTE: When set to **Enabled**, the **Enable Custom Backgrounds** and **Interval Between Backgrounds** options on the Room Schedule screen (described in [Display Customization \(on page 79\)](#)) are disabled.

6. Click **Save Changes** to apply any changes or click **Revert** to revert back to the previously used settings.

NOTE: For best practices on configuring the AM-200/AM-300 for use with Appspace visit docs.appspace.com.

AMPS

Click **AMPS** to configure the device's .AV Framework™ platform functionality. This section contains options for configuring system settings, controlling Crestron Fusion software operation, configuring the display device, configuring touch screen operation, adding and monitoring Zūm devices, managing the system's configuration, and viewing activity logs.

System

Click **System** to specify the room name, the local language setting, the time format, the date format, and manage the power settings.

AMPS Screen – System

The system is currently online.

System

System Settings

Room Name: AVF 87492

Language: English (English)

Time Format: 12 hour

Date Format: January 15, 2017

Save

Power Settings

Standby: Always On

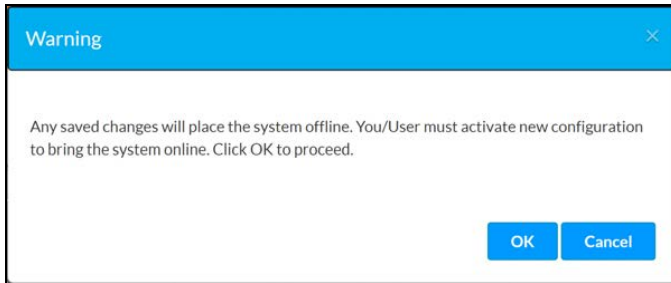
Day Of Week	Enabled	Display On	Display Off
Sunday	Enable	12:00 AM	11:59 PM
Monday	Enable	12:00 AM	11:59 PM
Tuesday	Enable	12:00 AM	11:59 PM
Wednesday	Enable	12:00 AM	11:59 PM
Thursday	Enable	12:00 AM	11:59 PM
Friday	Enable	12:00 AM	11:59 PM
Saturday	Enable	12:00 AM	11:59 PM

Save

System Settings

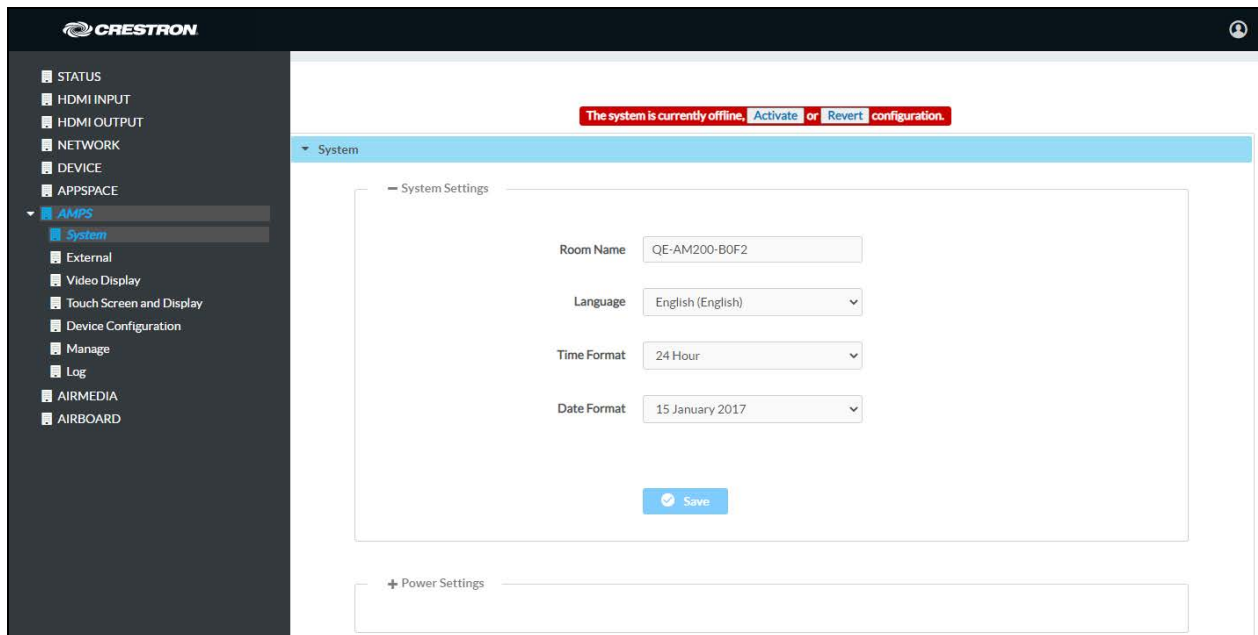
1. Enter the room name in the **Room Name** field.
2. Select the local language from the **Language** drop-down list.
3. Select the time format from the **Time Format** drop-down list (**12 hour** or **24 hour**).
4. Select the date format from the **Date Format** drop-down list.
5. Click **Save**. A warning message is displayed.

Warning Message



6. Click **OK** to continue or click **Cancel** to cancel.

AMPS Screen – System – System Offline



7. Click **Activate** to activate the new settings and confirm the activation or click **Revert** to undo the changed settings.

Power Settings

Configure power settings to manage the system's power usage.

1. Select one of the following modes from the **Standby** drop-down list.
 - **Always On** sets the following:

NOTE: **Always On** is the default setting.

- The display device will be on during business hours (defined in step 2).
- The touch screen will always be on.

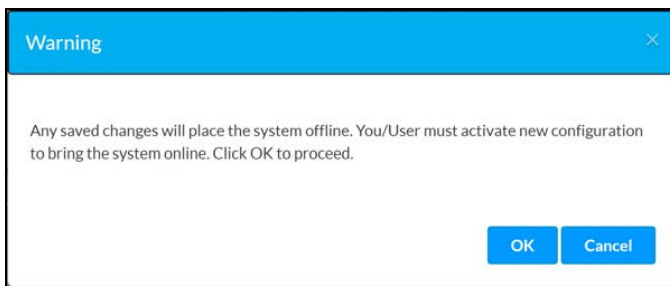
- Crestron Fusion power events will be ignored.
- During business hours, "Occupancy Vacant" events will be ignored.
- During business hours "Occupancy Occupied" events will turn the room on if the room is off.
- Outside of business hours, Occupancy events can turn the room on and off.
- Hard button power events will be allowed.
- HDMI sync and video route will turn the room on outside of business hours.
- Panel hard button will be active to turn off the display device and the touch screen will be blank.
- **Based on Occupancy** sets the following:
 - The connected occupancy sensor will be used to determine when the room is occupied or vacant.
 - When the room is occupied the system will be on.
 - When the room is vacant the system will be off.
 - If the display device is configured as a controlled display device, it will be on when the room is occupied and off when the room is vacant.
 - The touch screen will be on when the room is occupied and off when the room is vacant.
 - Crestron Fusion power events will not be ignored.
 - A detected video sync signal will turn on the room.
 - Connecting to the device by an AirMedia connection will not turn on the room.
- **Occupancy Based With Signage** sets the following:
 - The occupancy sensor will be used to determine when the room is occupied or vacant.
 - When the room is occupied the system will be on.
 - When the room is vacant, the system will be operating in standby mode during defined business hours and off outside of business hours (defined in step 2).
 - The display device will be on when the system is in standby mode and off when the system is off.
 - The touch screen will be on when the room is occupied and off when the room is vacant.
 - When in the standby mode, digital signage that is configured to run during standby mode will be displayed.
 - Crestron Fusion power events will not be ignored.

- Connecting an active HDMI input source will turn on the room.
- Connecting to the device by an AirMedia connection will not turn on the room.

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

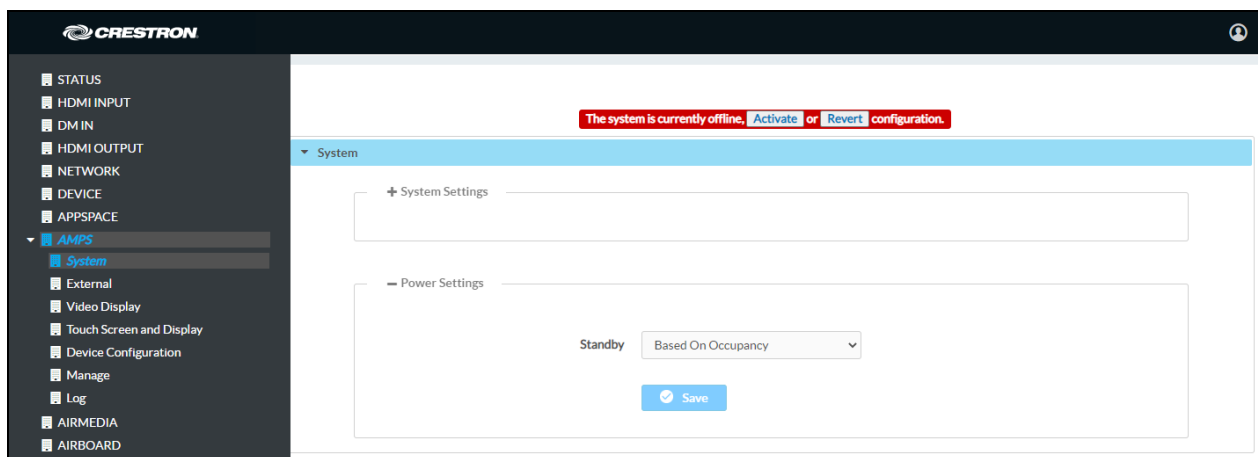
- For each day of the week, define business hours (**Always On** and **Occupancy Based With Signage** settings only).
 - For each day, set the **Enabled** setting to **Enable** to include the day in the business hours schedule. Set the day's **Enabled** setting to **Disabled** to remove the day from the business hours schedule.
 - Select a time from the day's **Display On** field to set the time the display device will turn on. To set the time, click the hour, then click the exact time.
 - Select a time from the day's **Display Off** field to set the time the display device will turn off. To set the off time, click the hour, then click the exact time.
- Click **Save**. A warning message is displayed.

Warning Message



- Click **OK** to continue or click **Cancel** to cancel.

AMPS Screen – System – System Offline



- Click **Activate** to activate the new settings and confirm the activation or click **Revert** to undo the changed settings.

The following table shows which operations are enabled for each **Standby** setting.

Standby Settings and Enabled Operations

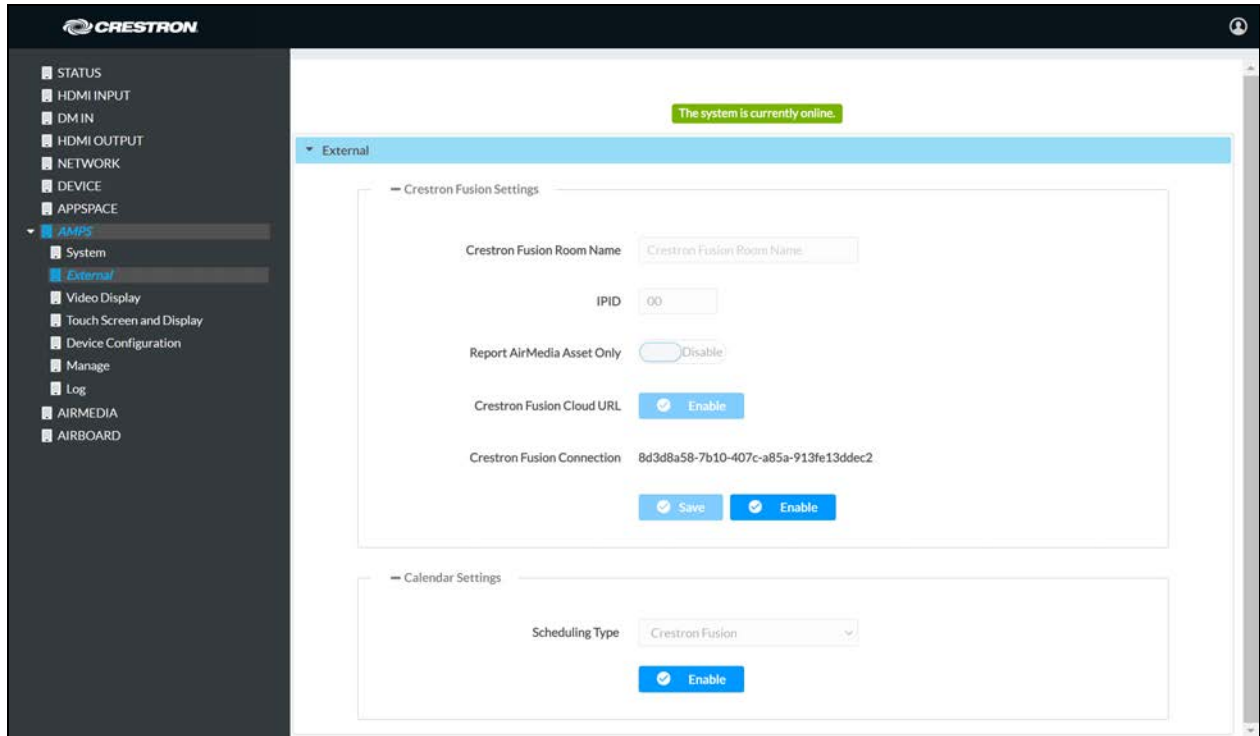
Operation	STANDBY SETTING		
	Always On	Occupancy Based	Occupancy Based With Signage
Always On	✓	✗	✗
Standby Off	✗	✗	✓
Allow Crestron Fusion Power On	✗	✓	✓
Allow Crestron Fusion Power Off	✗	✓	✓
Allow Video Sync Power On	✓	✓	✓
Allow Video Route Power On	✓	✓	✓
Allow Hard Button Power Off	✓	✓	✓
Allow Hard Button Power On	✓	✓	✓
Allow Fixed Schedule Power Control	✓	✗	✓
Allow Occupancy Power Control	✓*	✓	✓
Allow Display Back Light Control	✓	✓	✓
Allow Display Touch Activity Power On	✓	✓	✓

* After business hours.

External

The **External** screen displays the settings for operating with Crestron Fusion software and other calendar applications.

AMPS Screen – External

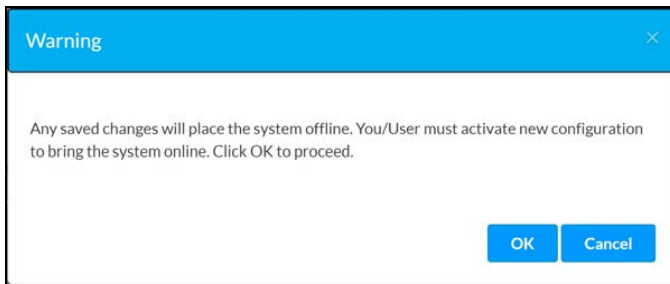


Crestron Fusion Settings

1. Enter the name to be used by the Crestron Fusion server in the **Crestron Fusion Room Name** field.
2. Enter the IP ID number to be used by the Crestron Fusion server in the **IPID** field.
3. (Optional) Set **Report AirMedia Asset Only** to **Enable** to allow an AM-200 or AM-300 to appear in Crestron Fusion with only AirMedia related settings. Set **Report AirMedia Asset Only** to **Disable** to allow all settings related to the AM-200/AM-300 and associated peripherals to appear in Crestron Fusion.

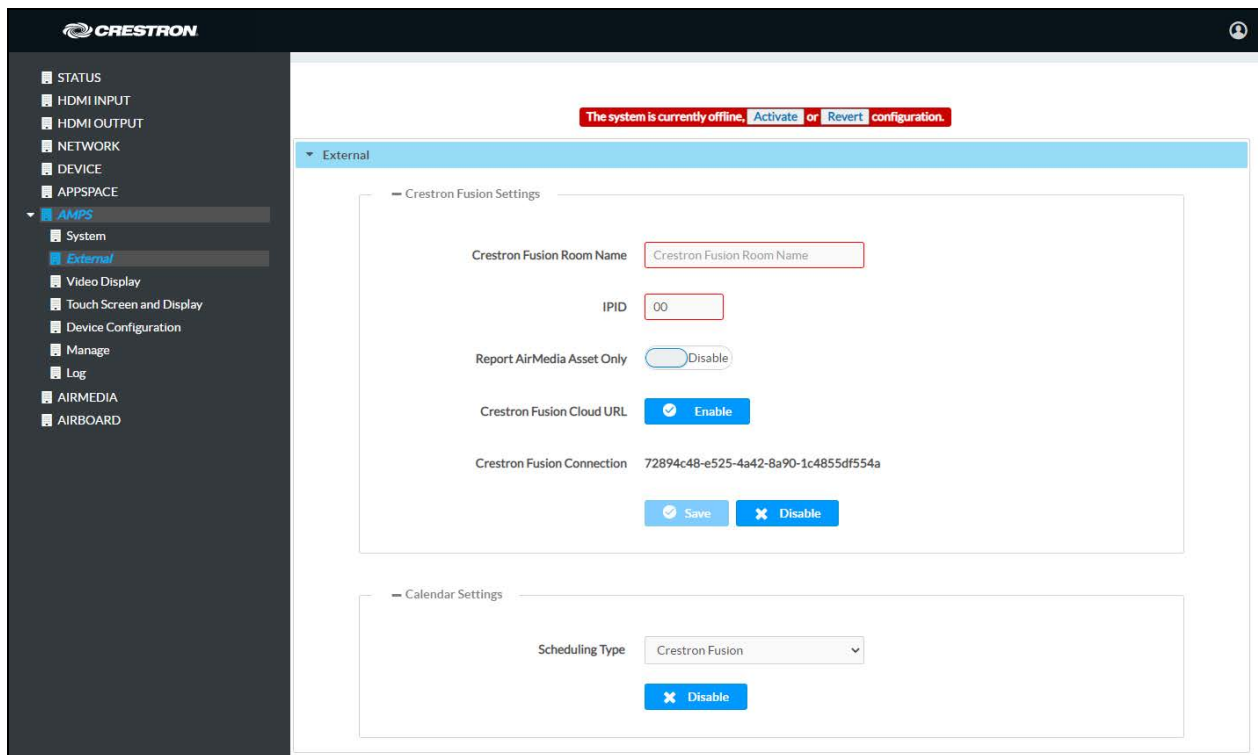
4. Click **Enable** in the **Crestron Fusion Cloud URL** field to allow autodiscovery by the Crestron Fusion server. A warning message is displayed.

Warning Message



5. Click **OK** to continue or click **Cancel** to cancel.

AMPS Screen – External – System Offline



6. Click **Activate** to activate the new settings and confirm the activation or click **Revert** to undo the changed settings.

Upon completion, the device should be brought into Crestron Fusion software as a processor. For details, refer to the Crestron Fusion help file.

To disable the connection to Crestron Fusion software, click **Disable**.

Calendar Settings

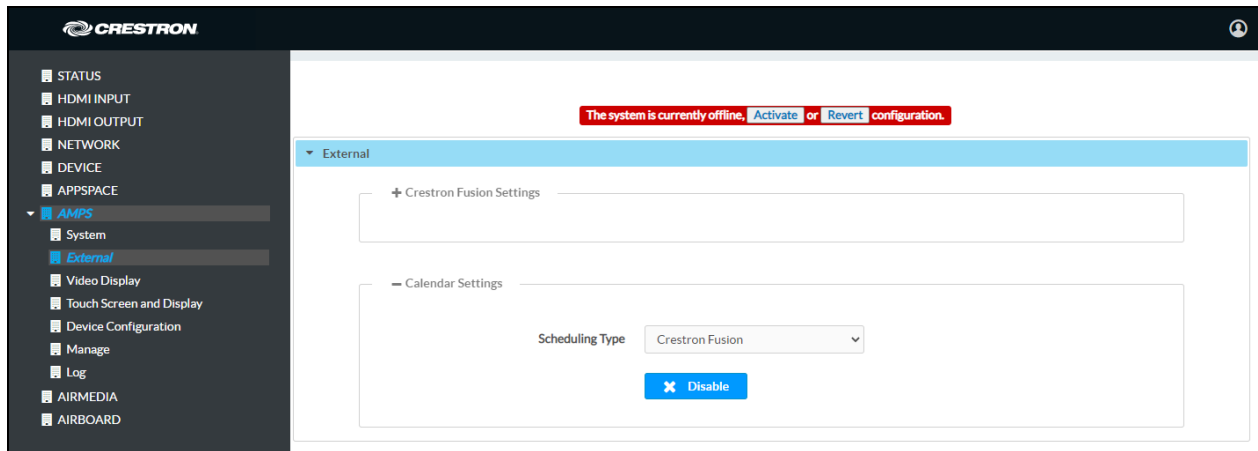
To configure the device to integrate with a calendar application, select the calendar type from the **Scheduling Type** drop-down list.

Crestron Fusion Software

Crestron Fusion is the default setting.

1. If switching from another calendar service, select **Crestron Fusion** from the **Scheduling Type** drop-down list.

AMPS Screen – External – System Offline



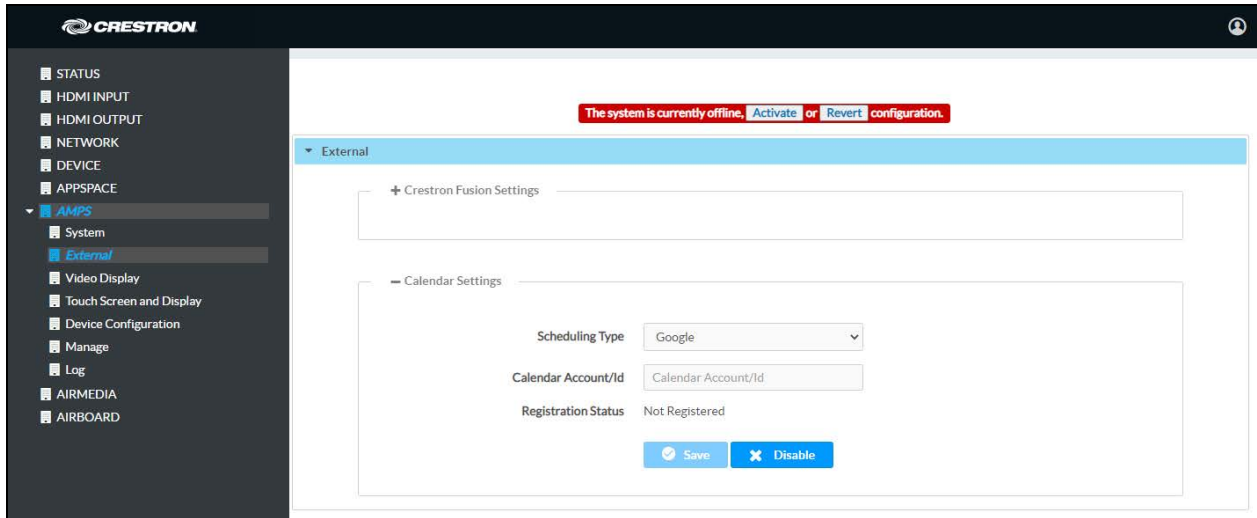
2. Click **Activate** to activate the new settings and confirm the activation or click **Revert** to undo the changed settings.

To disable the calendar, click **Disable**.

Google Calendar Service

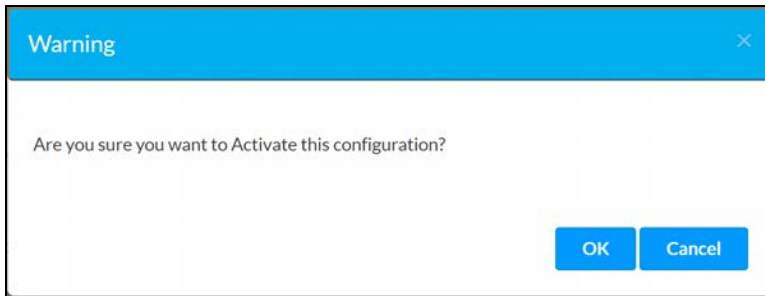
1. Select **Google** from the **Scheduling Type** drop-down list to use the Google Calendar™ application for calendar functions.

AMPS Screen – External – System Offline



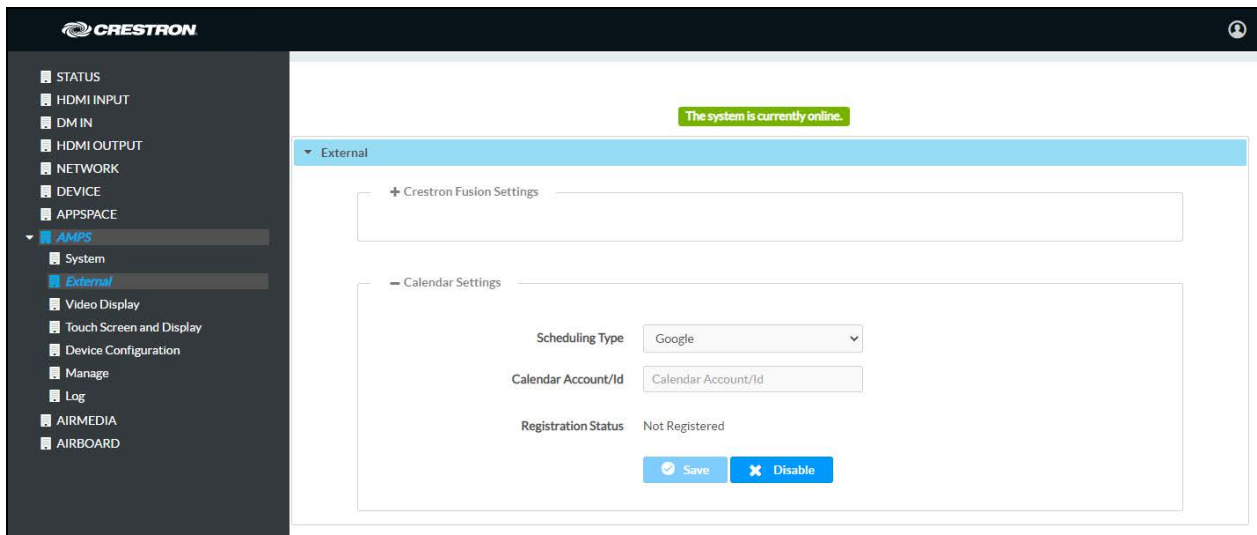
2. Click **Activate** at the top of the screen. A warning message is displayed.

Warning Message



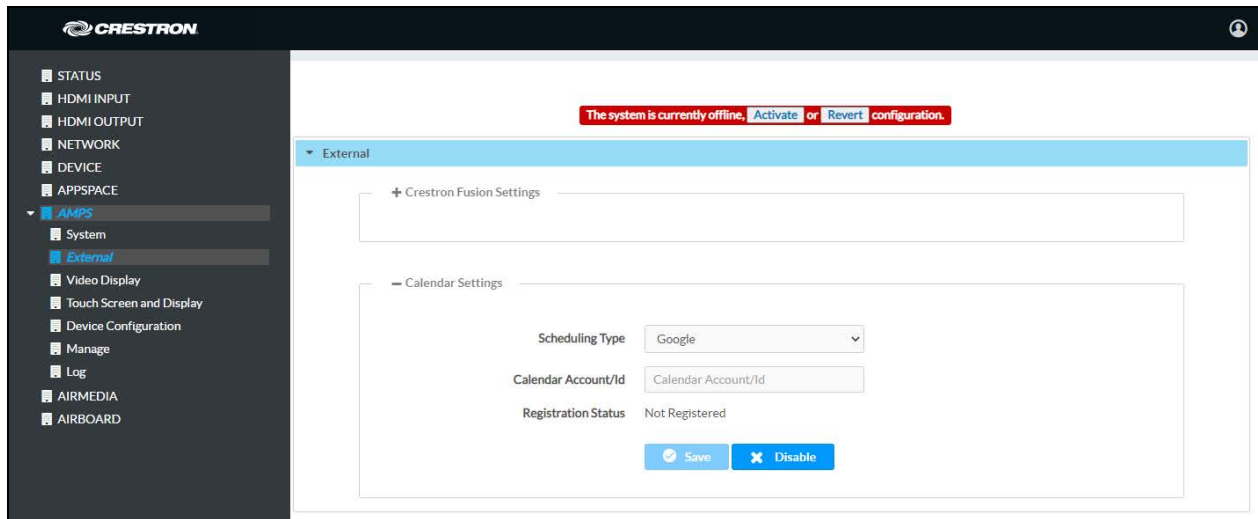
3. Click **OK** to activate the configuration.

Calendar Settings – Google Calendar



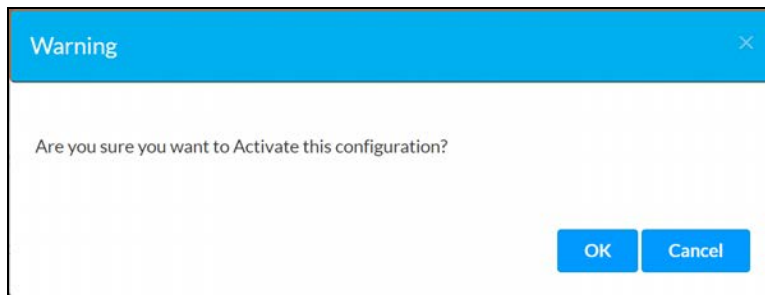
4. Enter the email address attached to the desired Google calendar in the **Calendar Account/ID** field and click **Save**.

AMPS Screen – External – System Offline



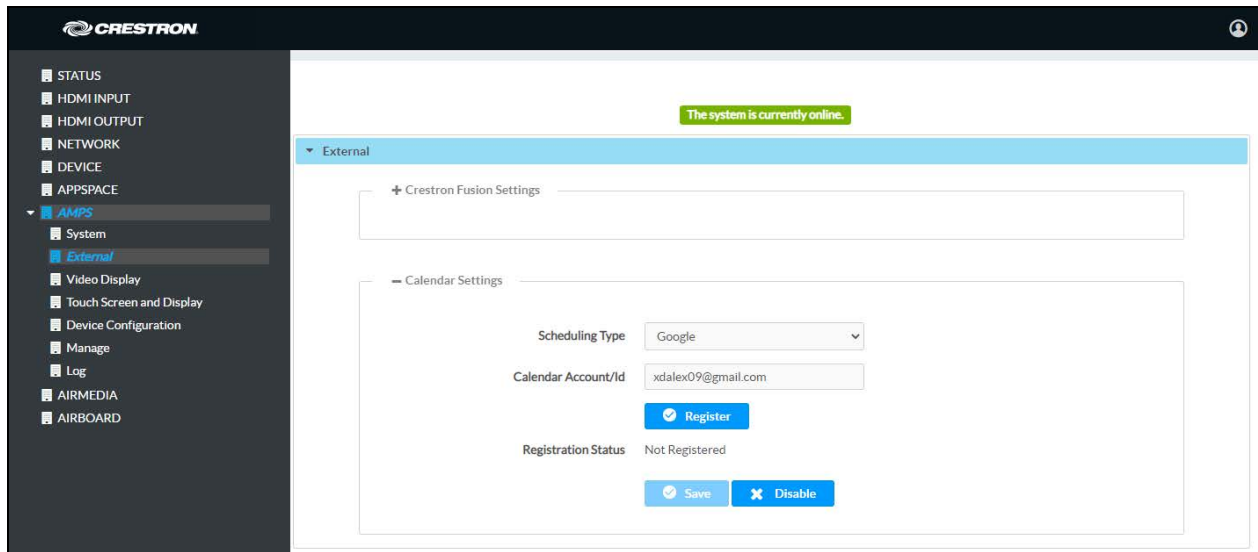
5. Click **Activate** at the top of the screen. A warning message is displayed.

Warning Message



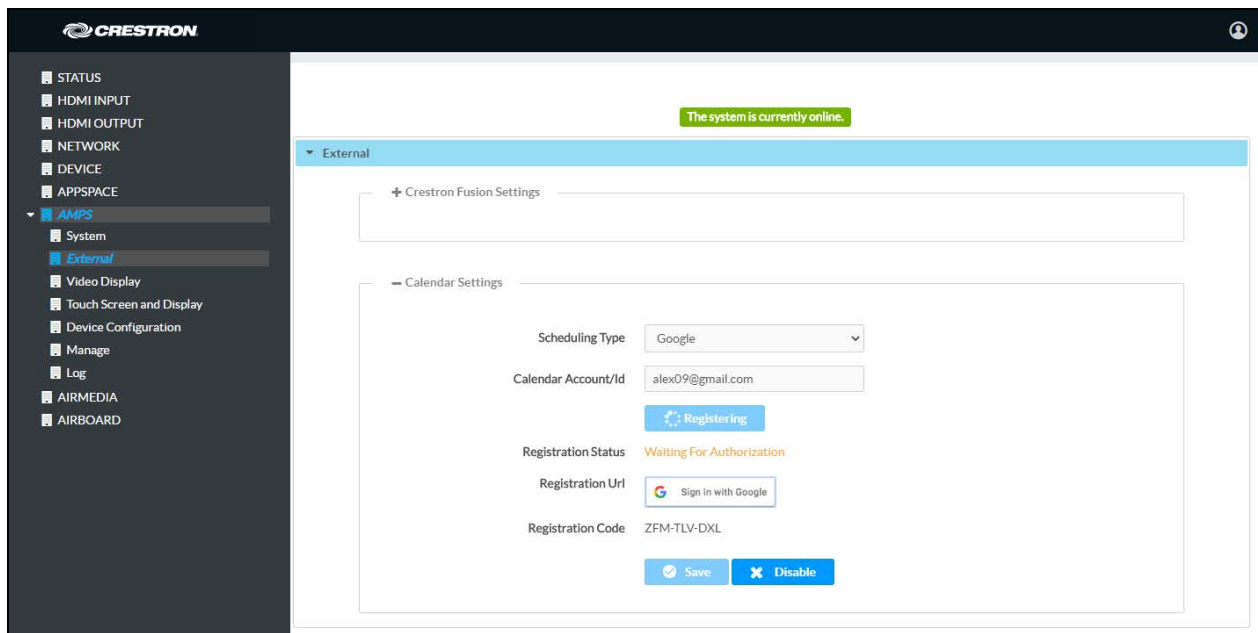
6. Click **OK** to activate the configuration.

Calendar Settings – Google Calendar



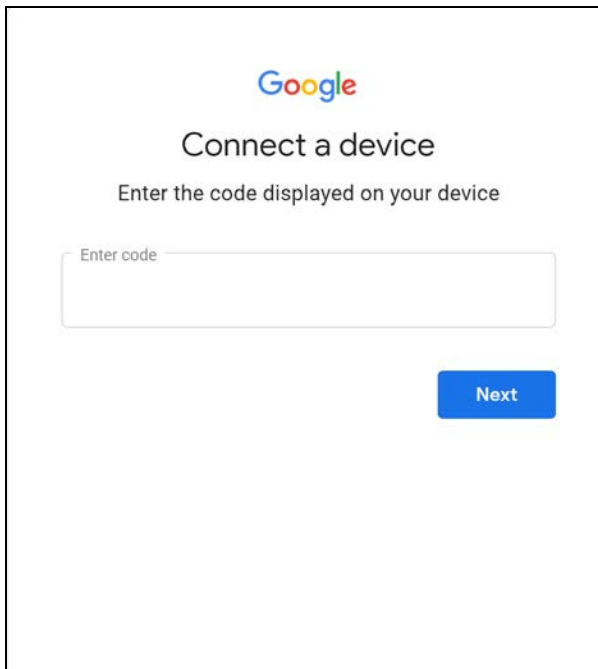
7. Click **Register**. The **Registration Status**, **Registration URL**, and **Registration Code** fields will appear.

Calendar Settings – Google Calendar



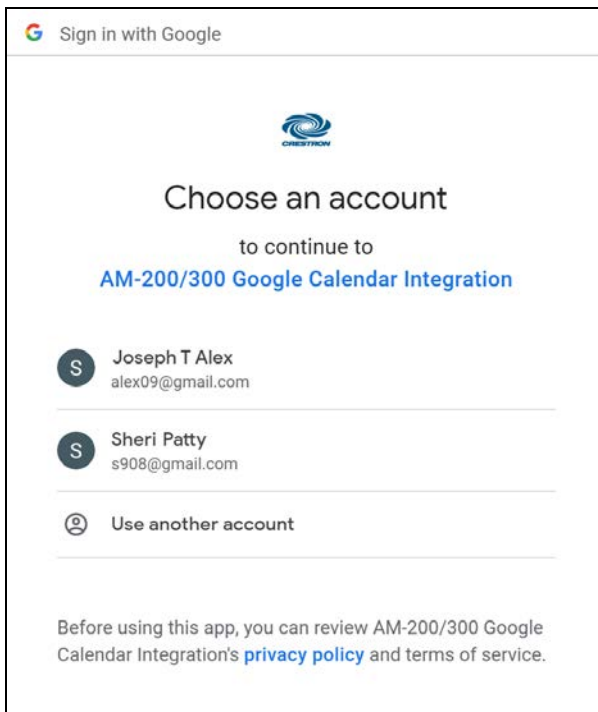
8. Highlight and copy the code in the **Registration Code** field to the clipboard.
9. Click **Sign in with Google**. A new web browser tab will open.

Connect a Device Screen



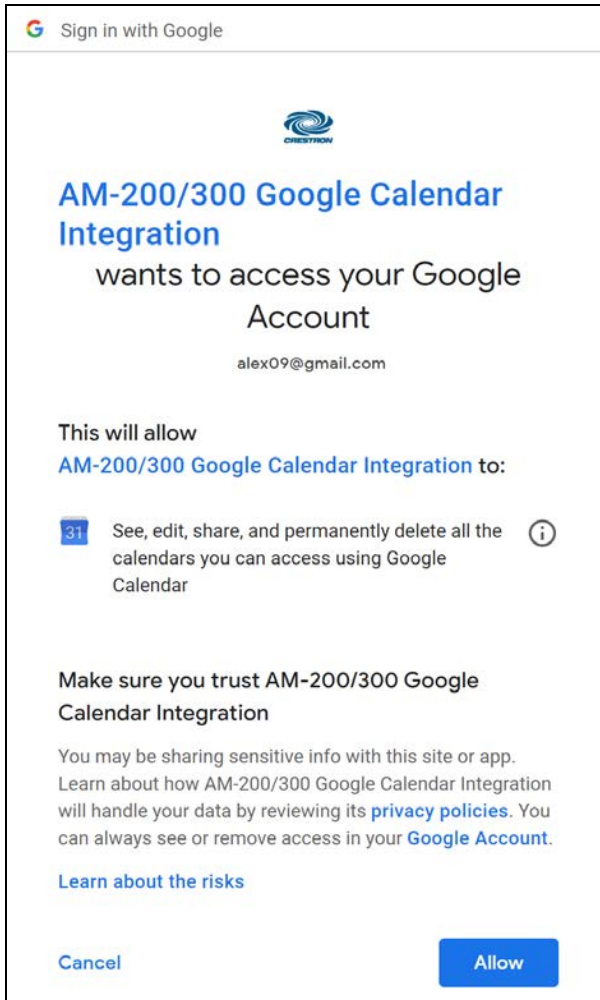
10. Paste the registration code in the **Enter code** field and click **Next**.

Choose an Account Screen



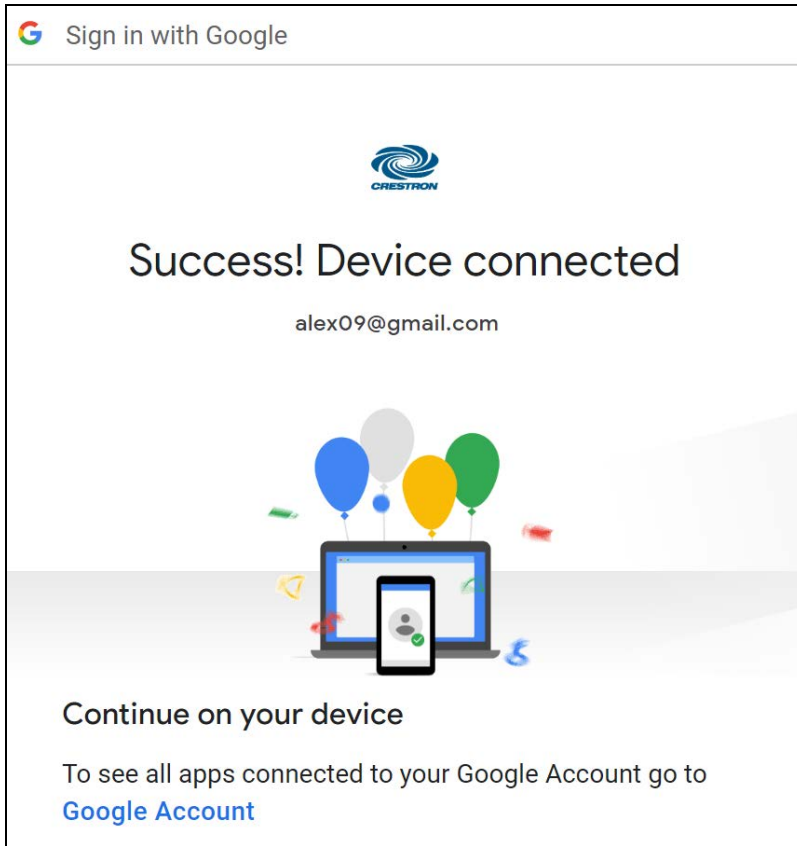
11. Click on an account and sign in with the login credentials.

Allow Access Screen

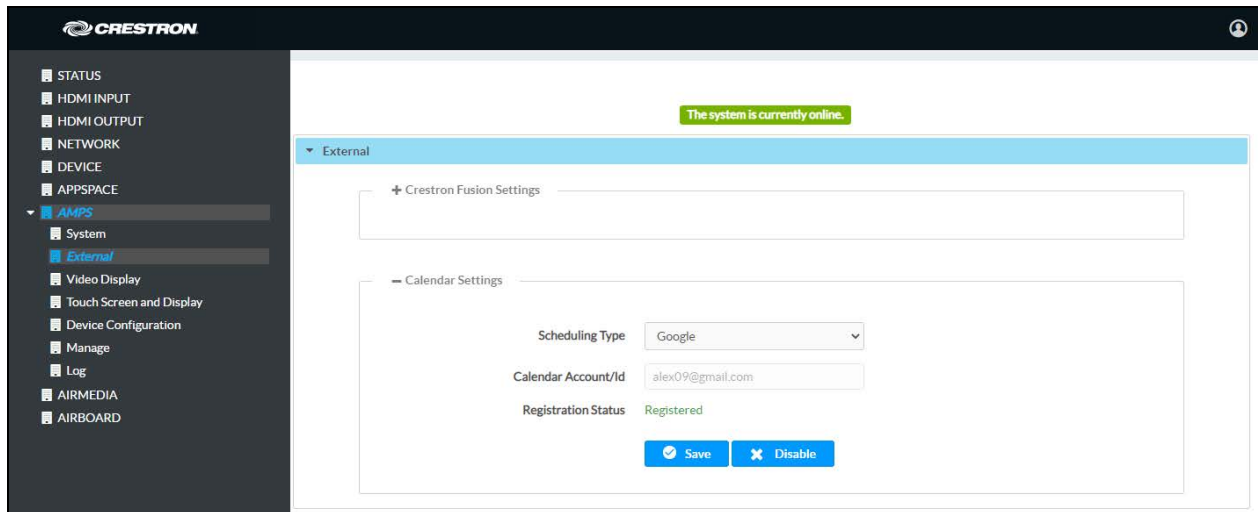


12. Click **Allow** to complete the process. A success message will be displayed, and the Google Calendar status will be updated.

Success Screen



Calendar Settings – Google Calendar

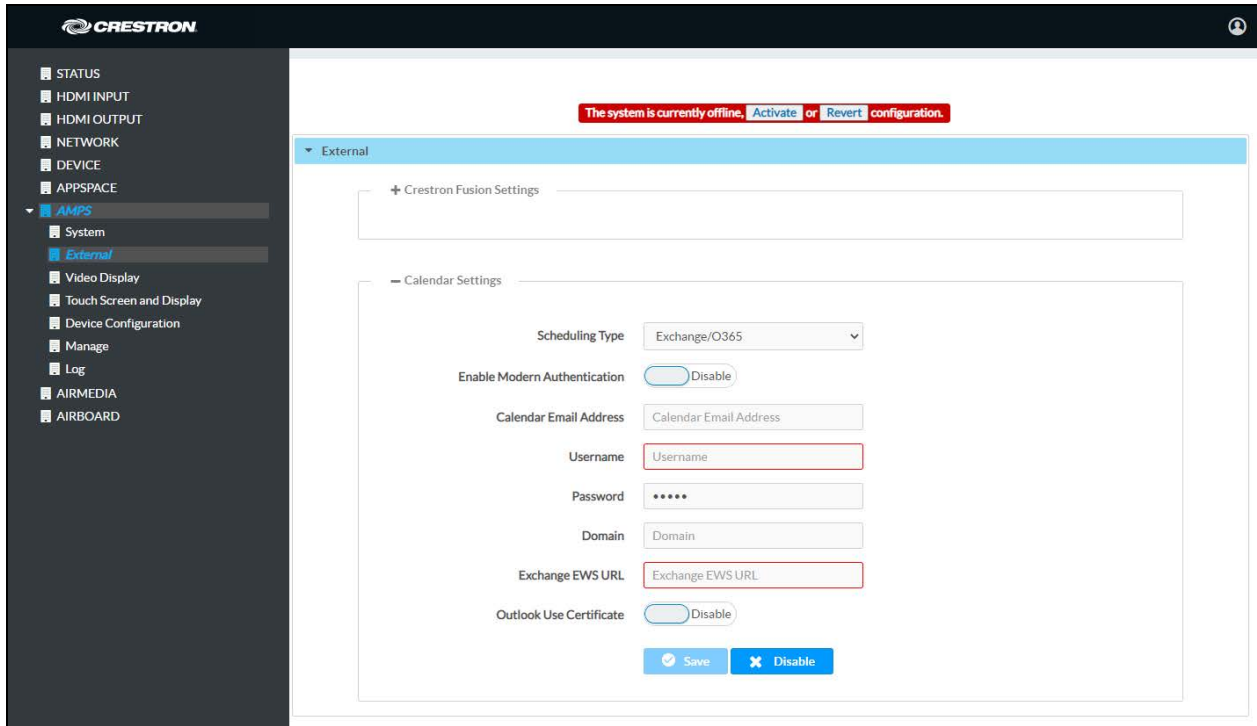


To disable the calendar, click **Disable** and follow the instructions for activating the configuration.

Microsoft Exchange Server and Microsoft 365 Software, Modern Authentication

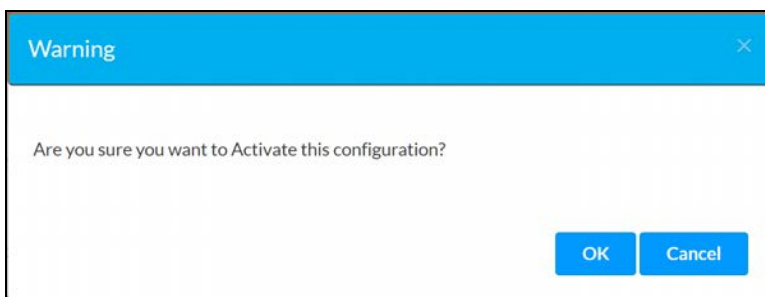
1. Select **Exchange/O365** to use Microsoft Exchange Server® or Microsoft 365 software for calendar functions.

AMPS Screen – External – System Offline



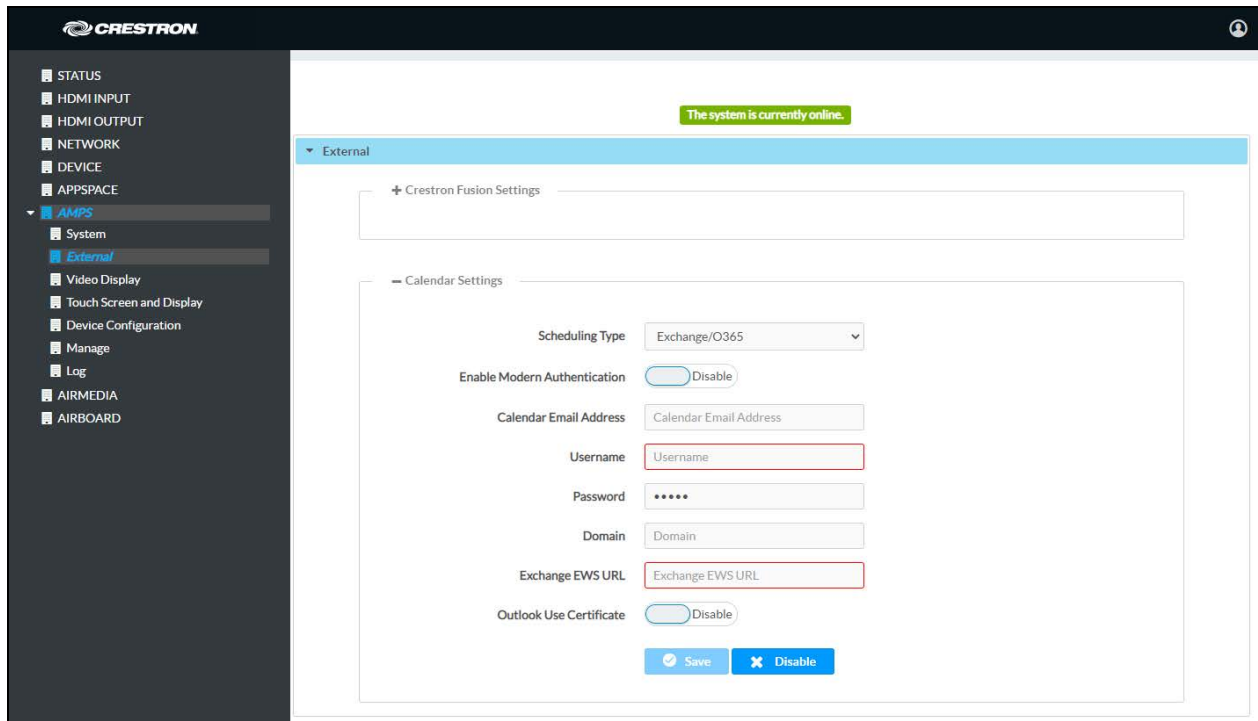
2. Click **Activate** at the top of the screen. A warning message is displayed.

Warning Message



3. Click **OK** to activate the configuration.

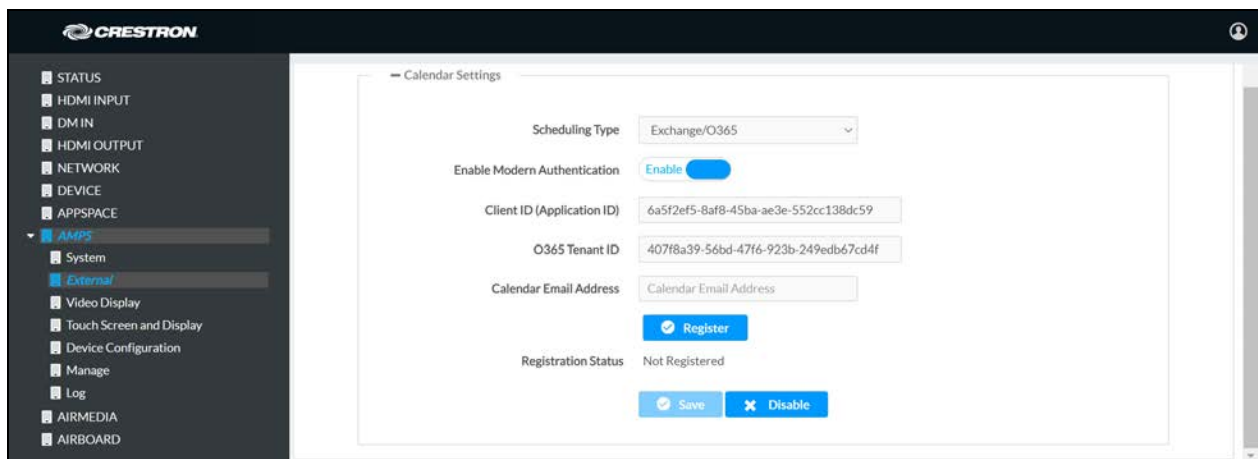
AMPS Screen – External – Calendar Settings – Exchange/O365 Calendar



4. Set the **Enable Modern Authentication** switch to **Enable** to use Modern Authentication.

NOTE: Consult with your IT administrator to configure the Azure® Active Directory service with an app registration for this integration. For more information, refer to [Appendix A: Enabling Modern Authentication for EWS \(on page 131\)](#).

Calendar Settings – Exchange/O365 – Modern Authorization



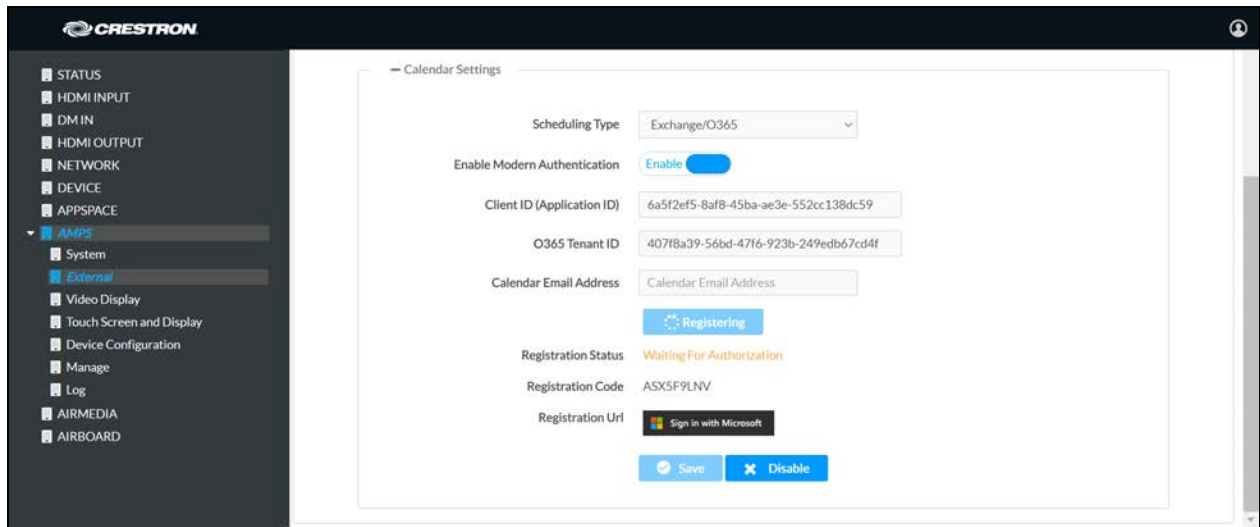
5. Enter a Client ID in the **Client ID (Application ID)** field.
6. Enter an O365/Microsoft 365 Tenant ID in the **O365 Tenant ID** field.

- (Optional) Enter the Calendar email address in the **Calendar email address** field.

NOTE: The Calendar email address is only required for accounts using impersonation.

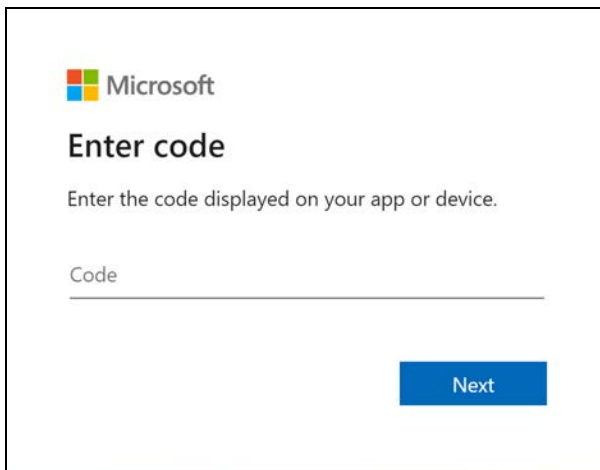
- Click **Save**. A code and a Microsoft icon will appear.

Calendar Settings – Exchange/O365 – Modern Authorization



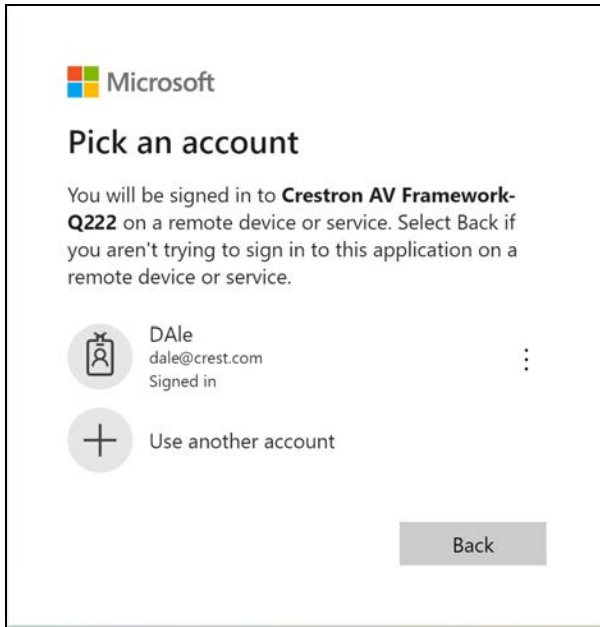
- Highlight and copy the code in the **Registration Code** field to the clipboard.
- Click the **Sign in with Microsoft**. A new web browser tab will open.

Enter Code Screen



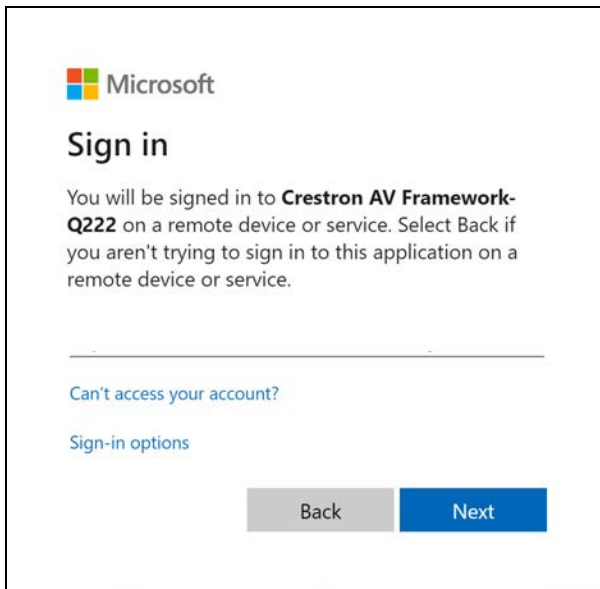
11. Paste the registration code in the **Code** field and click **Next**.

Pick an Account Screen



12. Click on the account to use.

Sign in Screen

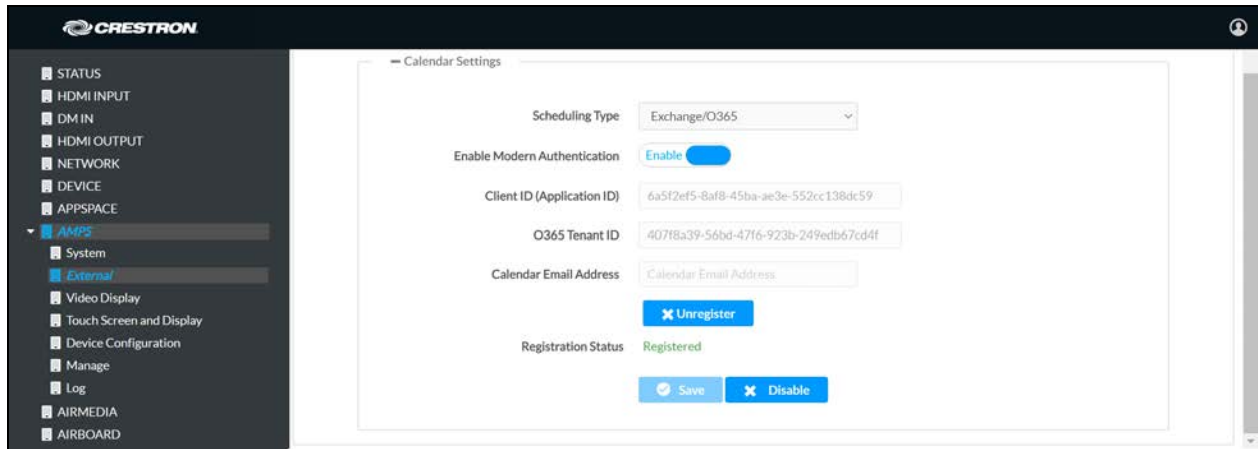


13. Sign in to the Microsoft 365 service. Once you are signed in, a confirmation message is displayed, and the Exchange/O365 Calendar status will be updated.

Confirmation Message



Calendar Settings – Exchange/O365 – Modern Authorization



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

To disable the calendar, click **Disable** and follow the instructions for activating the configuration.

Microsoft Exchange Server and Microsoft 365 Software, Modern Authentication Disabled

Calendar Settings – Exchange/O365 – Modern Authorization Disabled

The screenshot displays the 'External' settings page. Under the 'Calendar Settings' section, the 'Scheduling Type' is set to 'Exchange/O365'. The 'Enable Modern Authentication' toggle is currently set to 'Disable'. The 'Calendar Email Address' field is empty. The 'Username', 'Password', and 'Domain' fields are also empty. The 'Exchange EWS URL' field is empty. The 'Outlook Use Certificate' toggle is set to 'Enable'. Below this, there is an 'Upload Certificate' button. At the bottom of the settings area, there are 'Save' and 'Disable' buttons.

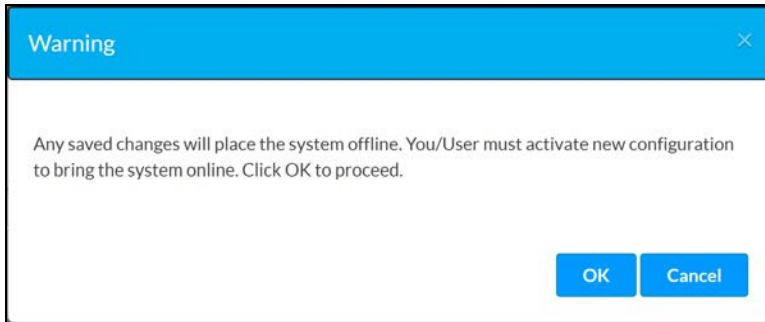
1. (Optional) Enter the Calendar email address in the **Calendar email address** field.

NOTE: The Calendar email address is required for accounts using impersonation.

2. Enter the user name in the **Username** field.
3. Enter the password in the **Password** field.
4. Enter the domain name used by the Exchange server in the **Domain** field.
5. Enter the URL of the Exchange server in the **Exchange EWS URL** field.
6. Set the **Outlook Use Certificate** switch to **Enable** to use an Outlook® certificate. Otherwise, set the switch to **Disable**.
 - a. Click **Upload**.
 - b. Navigate to the location of the firmware file.
 - c. Select the file to use and click **Open**.

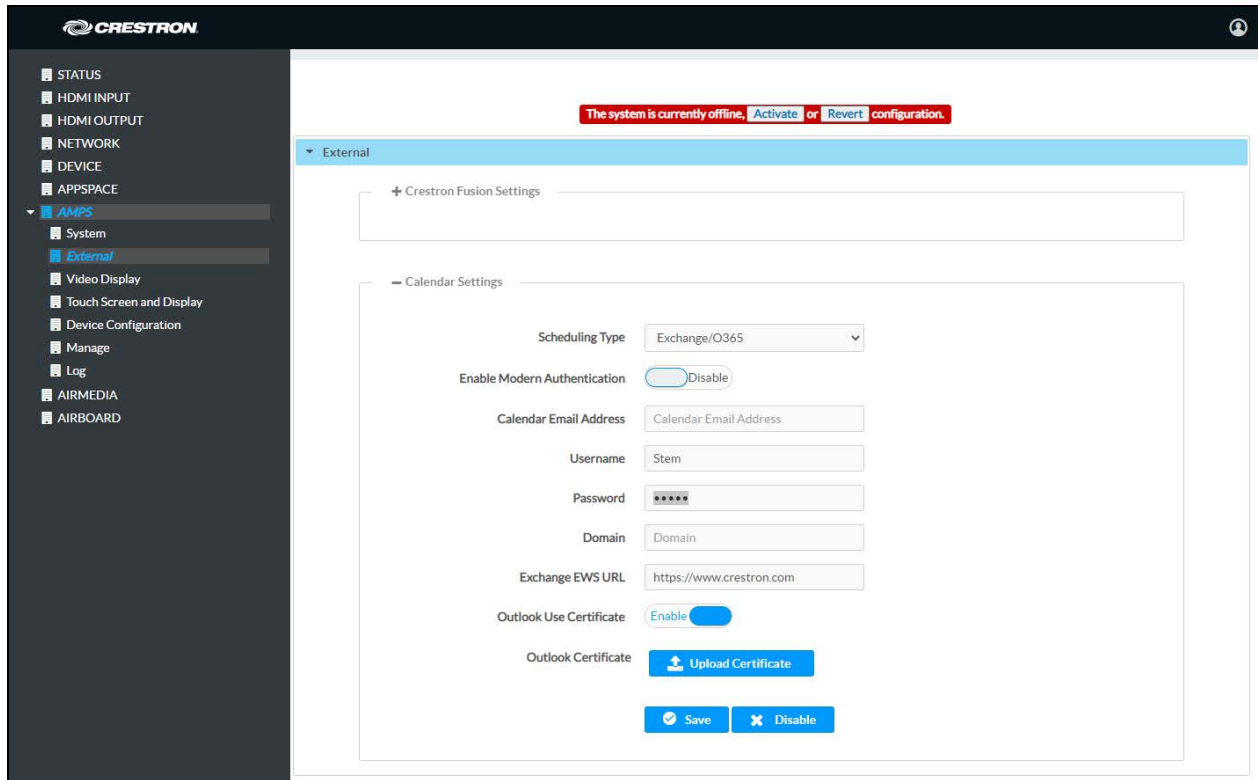
- Click **Save**. A warning message is displayed.

Warning Message



- Click **OK** to proceed or **Cancel** to cancel.

AMPS Screen – External – System Offline



- Click **Activate** to activate the new settings and confirm the activation or click **Revert** to undo the changed settings.

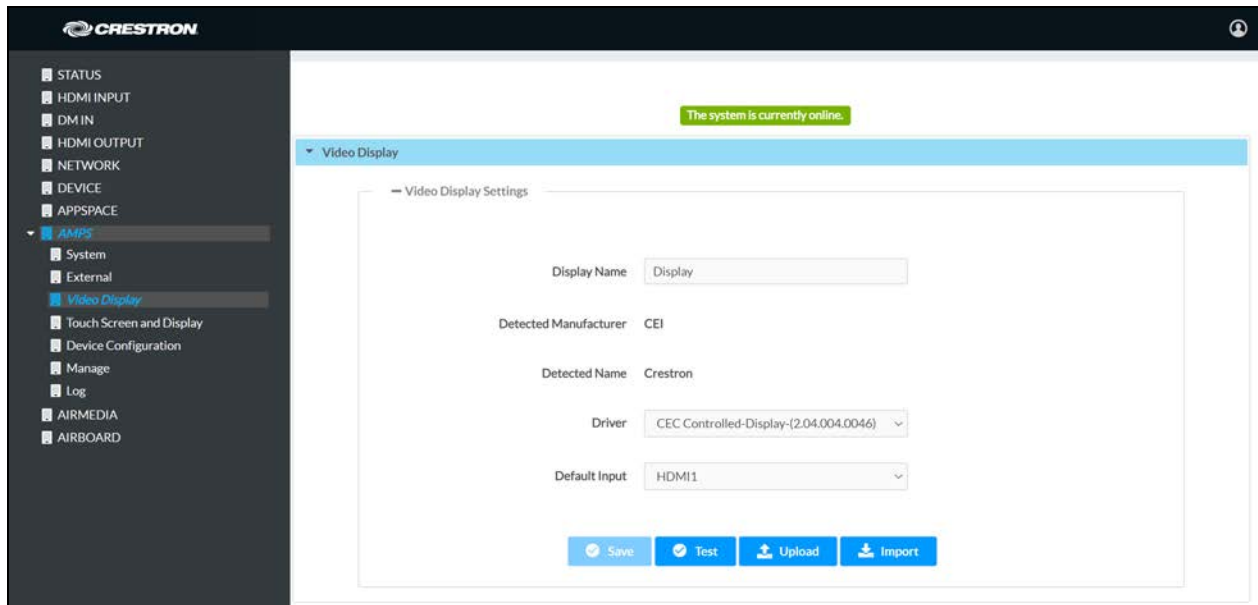
To disable the calendar, click **Disable** and follow the instructions for activating the configuration.

For more information, refer to Answer ID 5830 in the Online Help on the Crestron website (www.crestron.com/onlinehelp).

Video Display

The **Video Display** screen configures the device for operation with the display device. Support for CEC, Crestron Connected®, IP, serial, and infrared profiles are built in.

AMPS Screen – Video Display



Auto Detected Display

Configure the AM-200/AM-300 to work with a display device.

1. In the **Display Name** field, enter a name for the display device.
2. In the **Driver** drop-down list, select the driver for the display device.
3. Depending on the detected manufacturer, different controls are displayed. Complete the required fields to use the selected display.
4. Click **Save** to save the settings.
5. Click **Test** to display controls for testing the control commands.

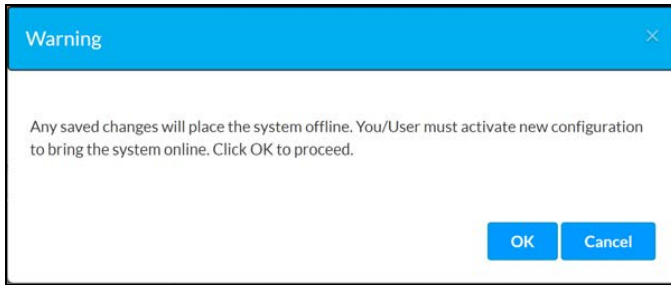
Upload a Custom Driver File

If the display device has a custom driver file, it can be uploaded to the device.

1. Click **Upload**.
2. Navigate to the location of the display's device driver file.
3. Select the file and click **Open**.

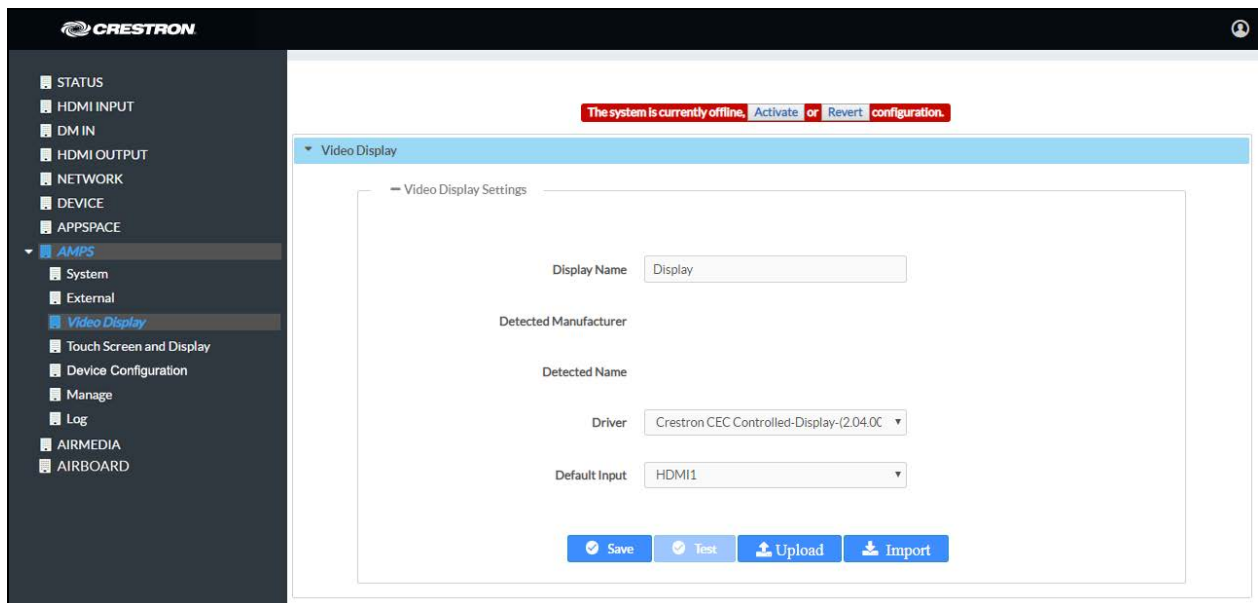
- Click **Save**. A warning message is displayed.

Warning Message



- Click **OK** to proceed or **Cancel** to cancel.

AMPS Screen – Video Display, driver selected



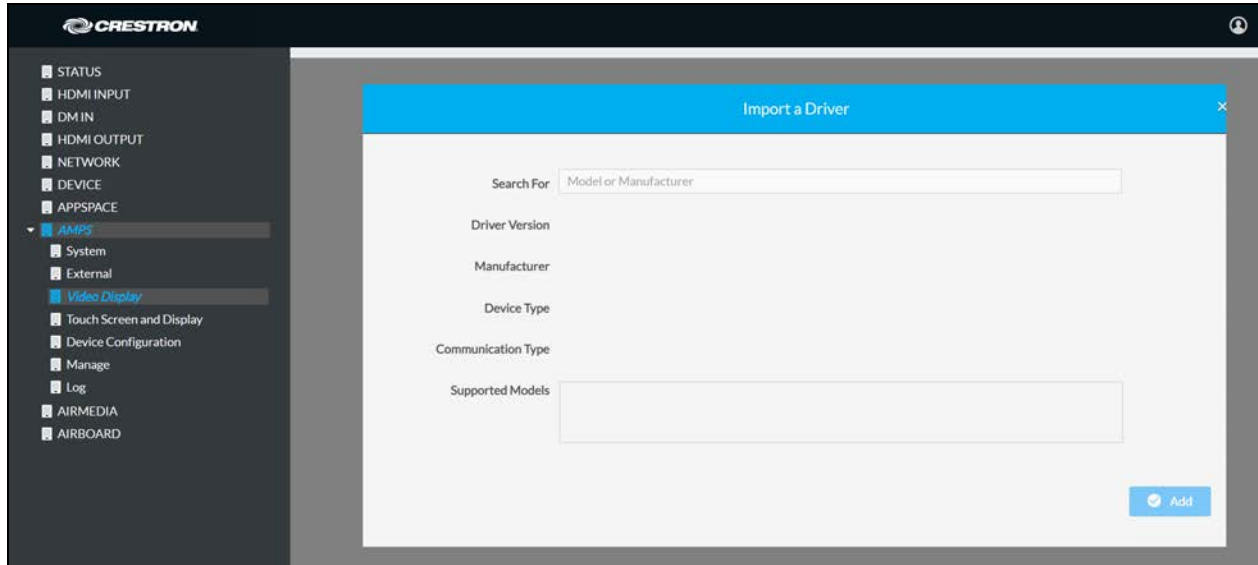
- Click **Activate** to activate the new settings and confirm the activation or click **Revert** to undo the changed settings.

Import a Driver File

You can search Crestron's cloud-based driver database for a specific driver.

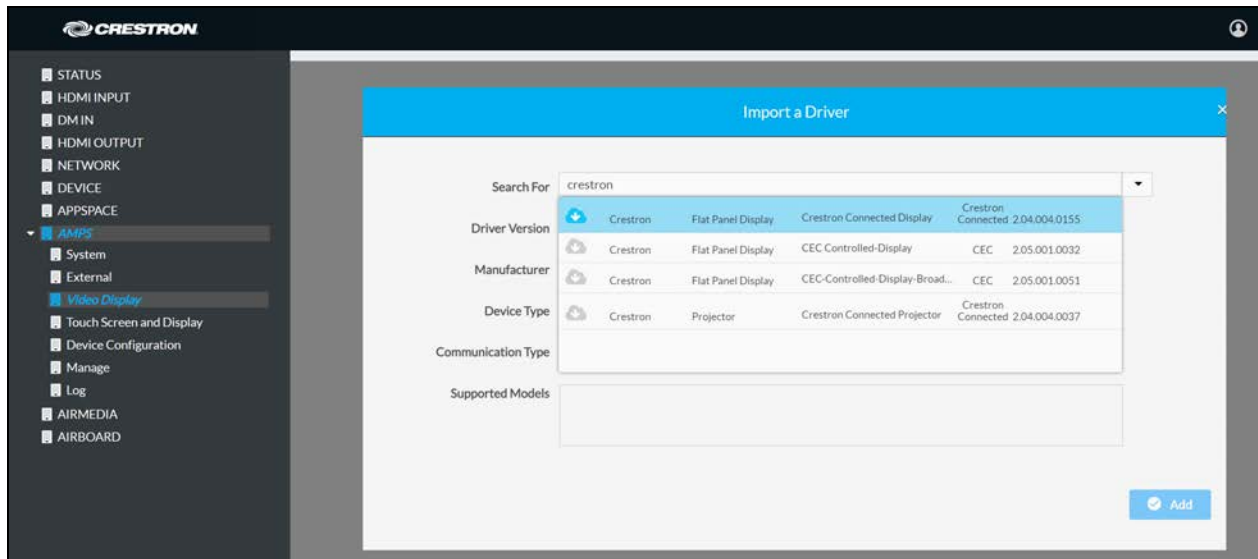
1. Click **Import**. The **Import a Driver** screen is displayed.

Import a Driver Screen



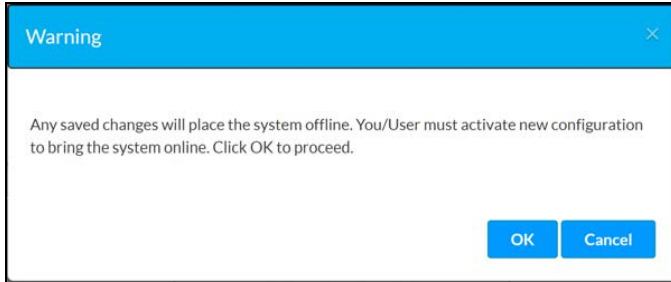
2. Enter a model or manufacturer name in the **Search For** field. Results are displayed in a drop down list from the **Search For** field.

Import a Driver Screen, Search Results



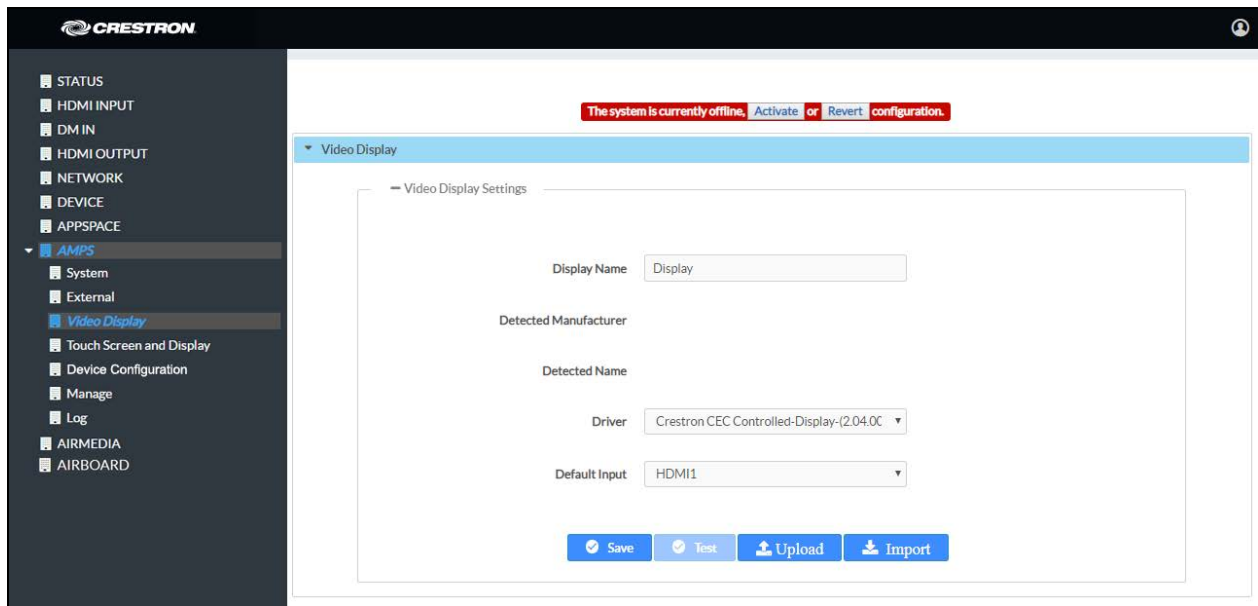
3. Click the desired driver from the drop-down list.
4. Click **Add** to add the driver to the device. The screen closes and the driver is selected for the display device.
5. Click **Save**. A warning message is displayed.

Warning Message



6. Click **OK** to proceed or **Cancel** to cancel.

AMPS Screen – Video Display, driver selected



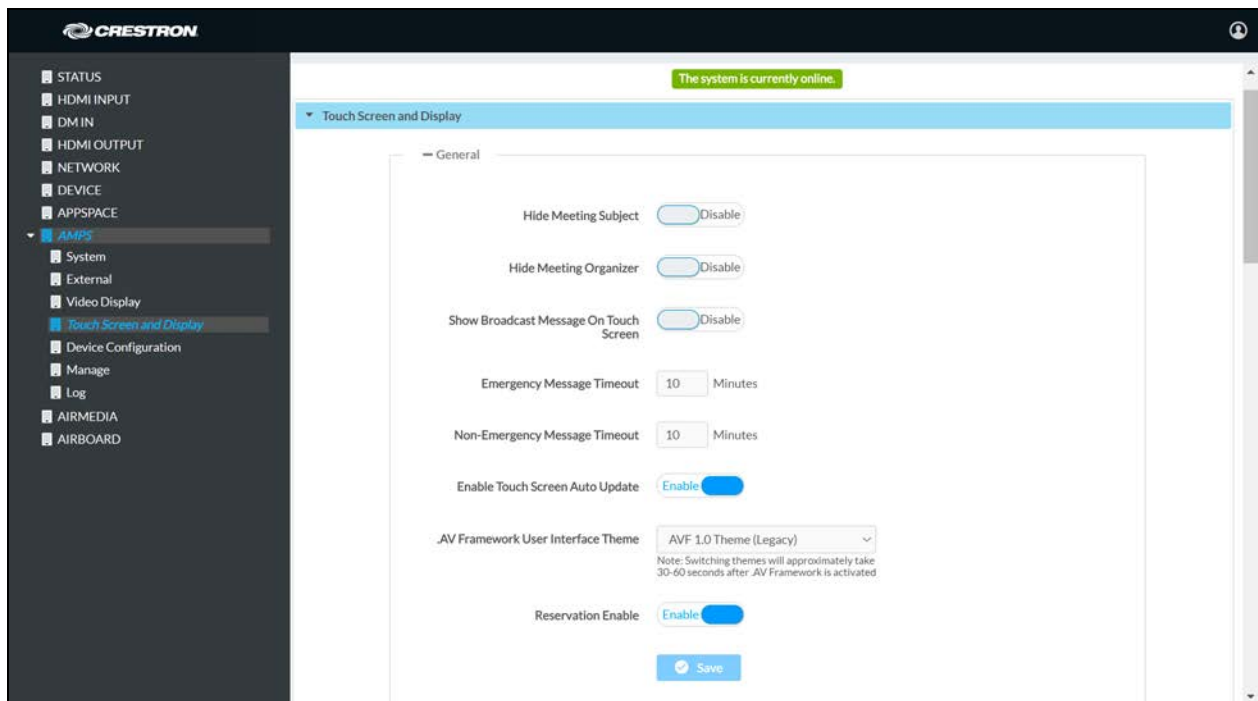
7. Click **Activate** to activate the new settings and confirm the activation or click **Revert** to undo the changed settings.

Touch Screen and Display

Click **Touch Screen and Display** to customize the function and appearance of the touch screen and the display device.

General

AMPS Screen – Touch Screen and Display – General



The General section specifies what information is shown on the touch screen and display device.

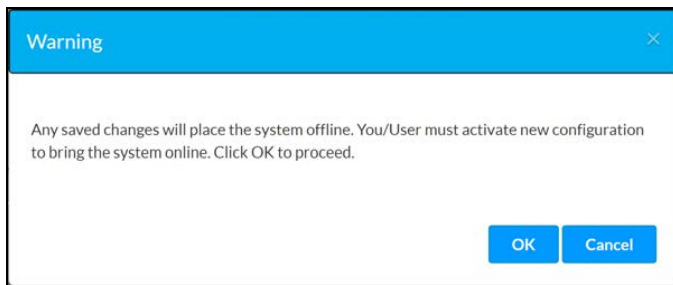
- Set **Hide Meeting Subject** to **Disable** to have the meeting's subject shown. To hide the meeting's subject, set **Hide Meeting Subject** to **Enable**.
- Select **Hide Meeting Organizer** to **Disable** to have the meeting's organizer shown. To hide the meeting's organizer, set **Hide Meeting Organizer** to **Enable**.
- Set **Show Broadcast Message on Touch Screen** to **Enable** to show broadcast messages on the touch screen (broadcast messages are automatically shown on the display device). To prevent broadcast messages from showing on the touch screen, set **Show Broadcast Message on Touch Screen** to **Disable**.
- Enter the number of minutes an emergency broadcast message is displayed in the **Emergency Broadcast Timeout** field.

NOTE: Emergency broadcasts are sent from Crestron Fusion. For more information on emergency broadcasts, refer to the [Crestron Fusion® Software SSI Model Reference Guide](#) (Doc. 7898).

- Enter the number of minutes a non-emergency broadcast message is displayed in the **Non-Emergency Broadcast Timeout** field.
- Set **Enable Touch Screen Auto Update** to **Enable** to allow project files to be pushed to the touch screen from the cloud automatically. To prevent the touch screen's project files from updating automatically, set **Enable Touch Screen Auto Update** to **Disable**.
- Select the desired theme for touch screens and displays from the **.AV Framework User Interface Theme** drop-down list.
- Set **Reservation Enable** to **Enable** to allow calendar reservations from a touch screen. To disable the calendar reservation capability on a touch screen, set **Reservation Enable** to **Disable**.

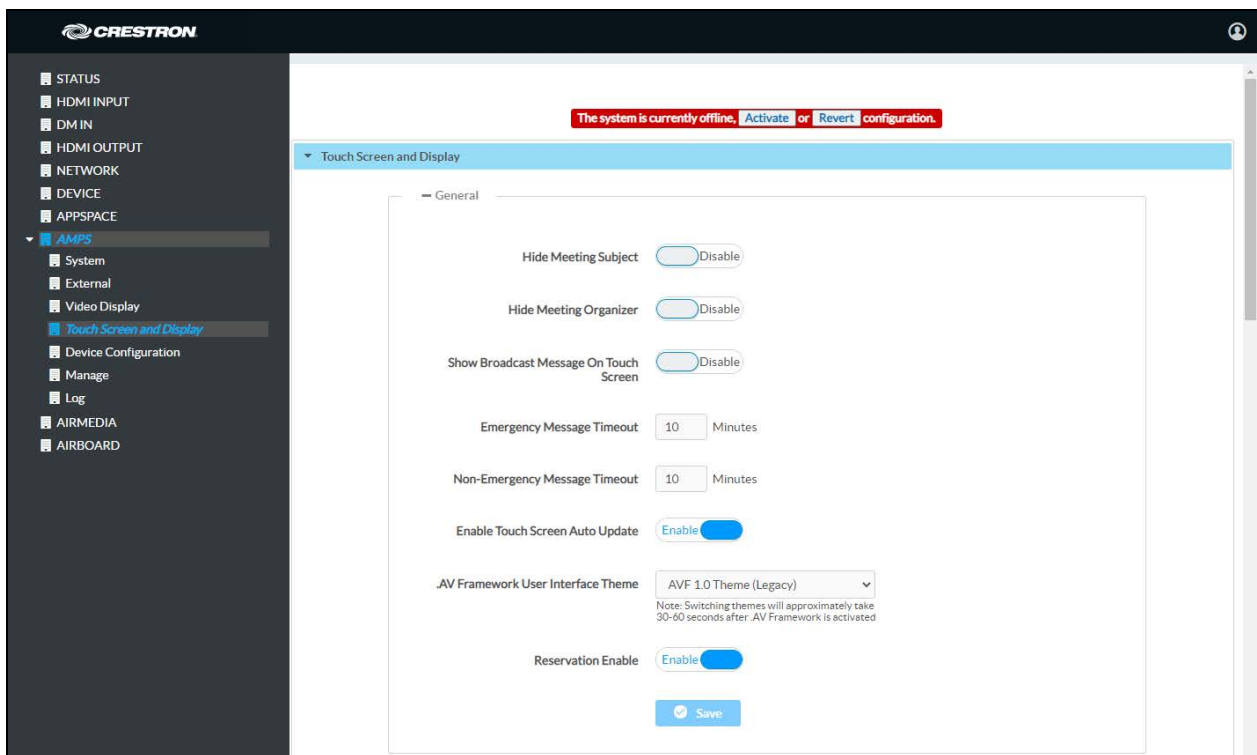
When all changes are made, click **Save**. A warning message is displayed.

Warning Message



1. Click **OK** to proceed or **Cancel** to cancel.

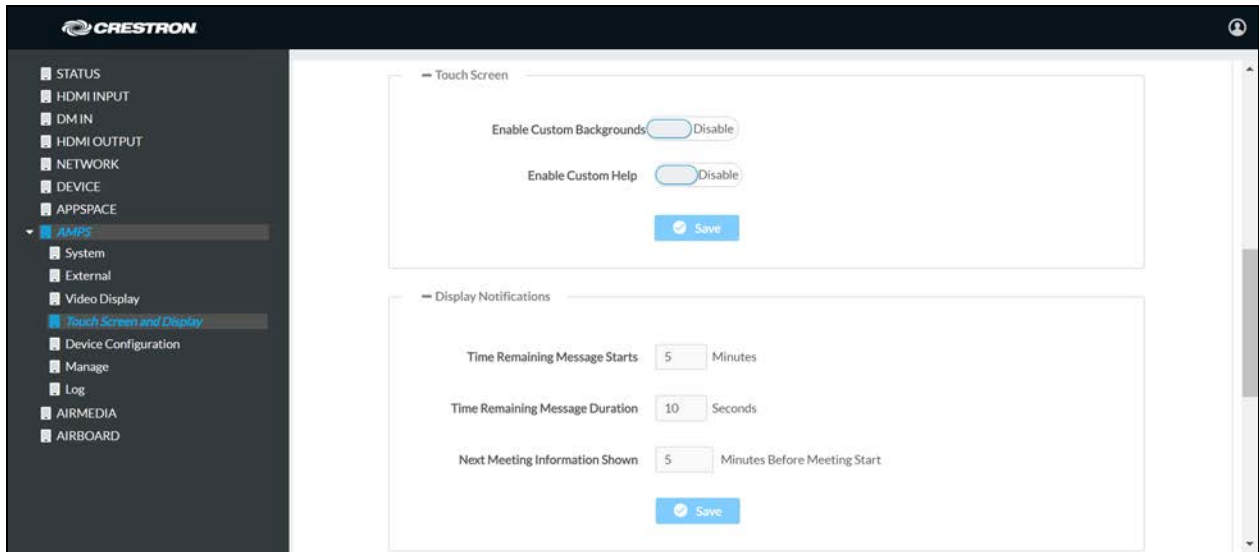
AMPS Screen – Touch Screen and Display – General



2. Click **Activate** to activate the new settings and confirm the activation or click **Revert** to undo the changed settings.

Touch Screen

AMPS Screen – Touch Screen and Display – Touch Screen

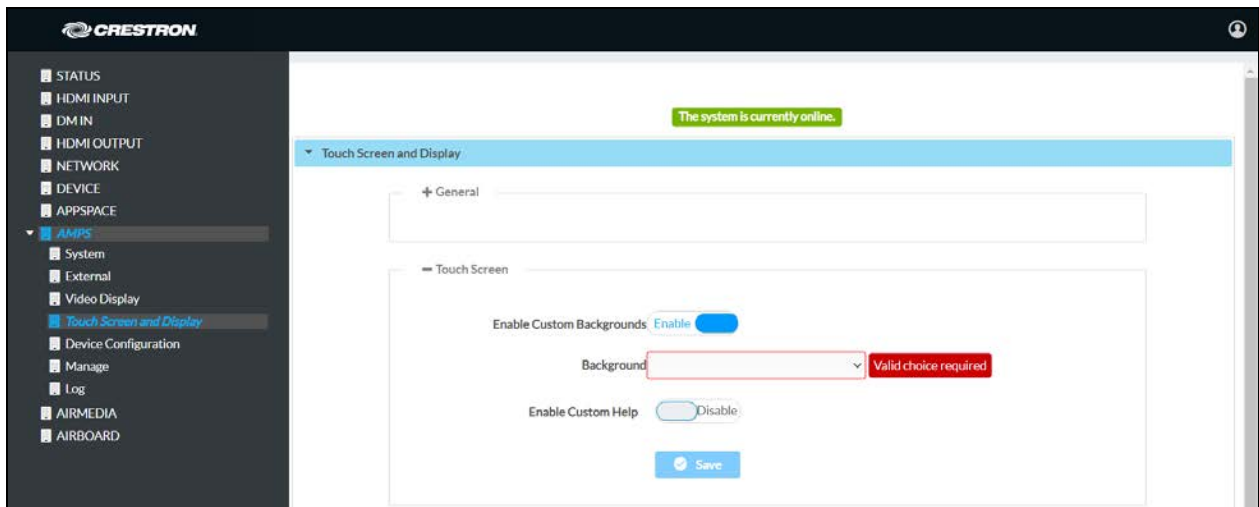


Background Images

Preloaded background images can be shown on the device's connected touch screen.

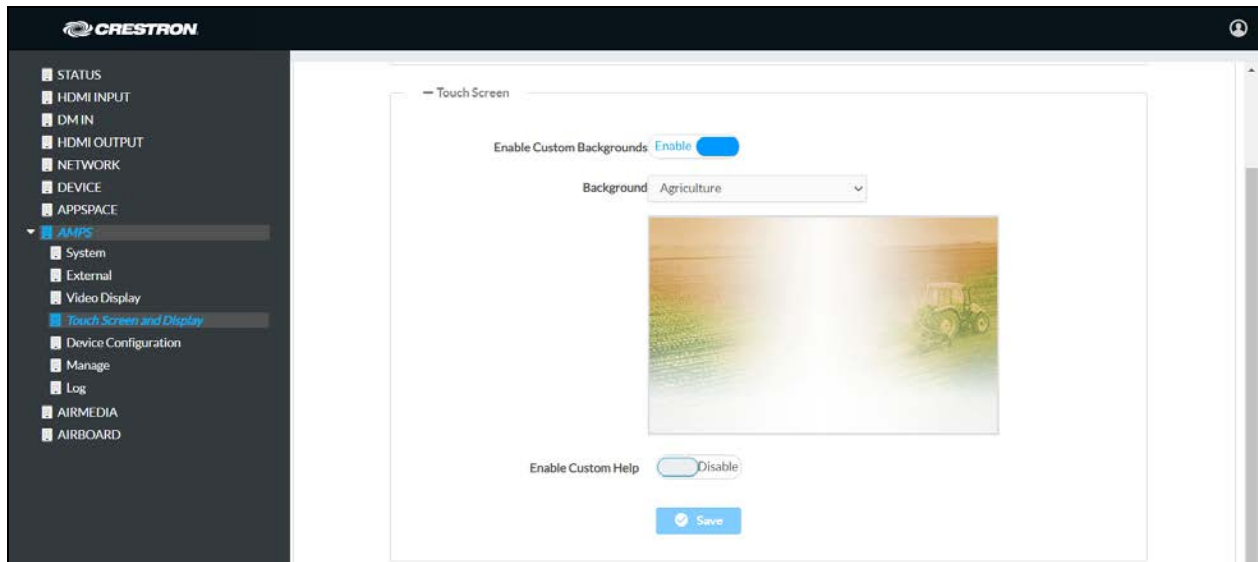
1. Set **Enable Custom Backgrounds** to **Enable**.

AMPS Screen – Touch Screen and Display – Touch Screen



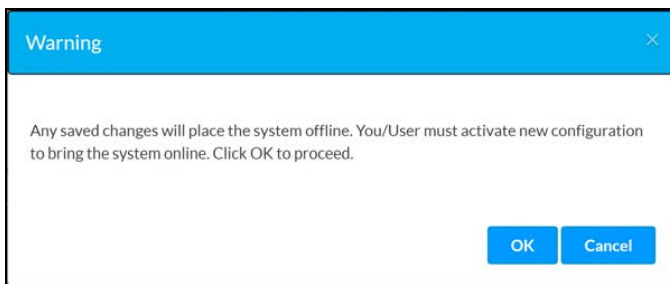
2. Select an image from the **Background** drop-down list.

AMPS Screen – Touch Screen and Display – Touch Screen



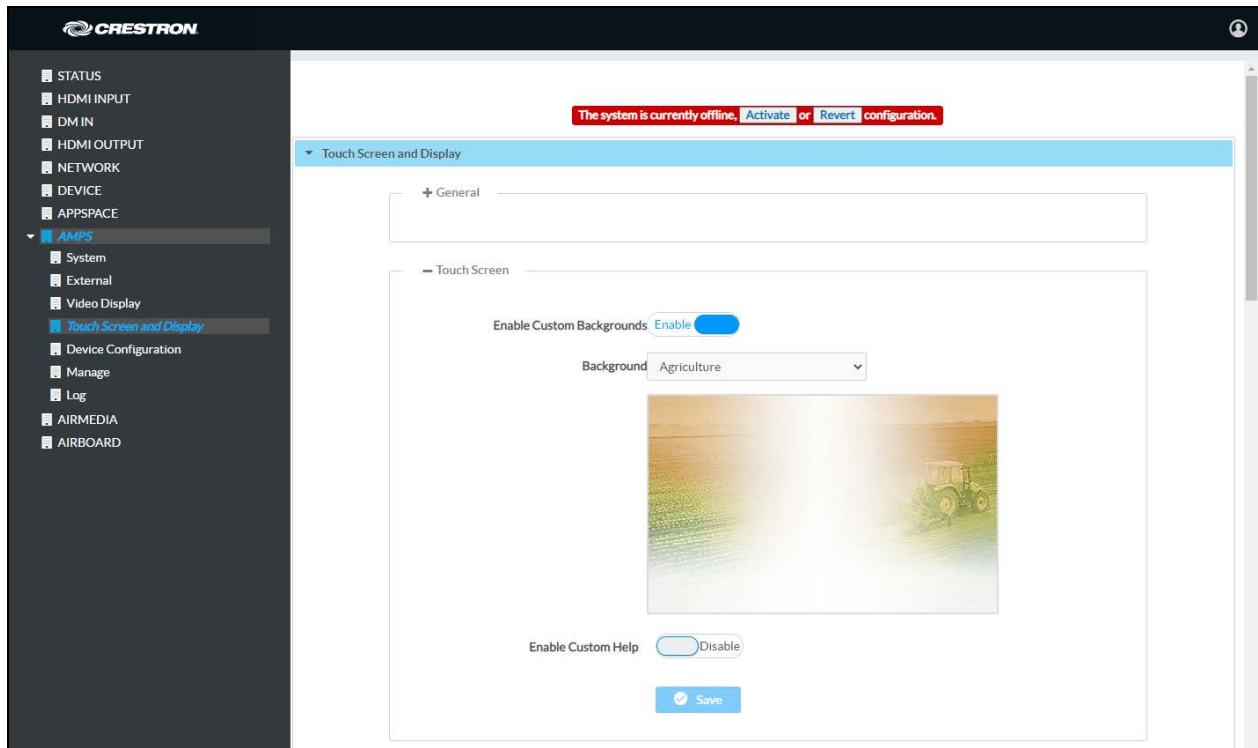
3. Click **Save**. A warning message is displayed.

Warning Message



4. Click **OK** to proceed or **Cancel** to cancel.

AMPS Screen – Touch Screen and Display – Touch Screen



5. Click **Activate** to activate the new settings and confirm the activation or click **Revert** to undo the changed settings.

Custom Help Page Image

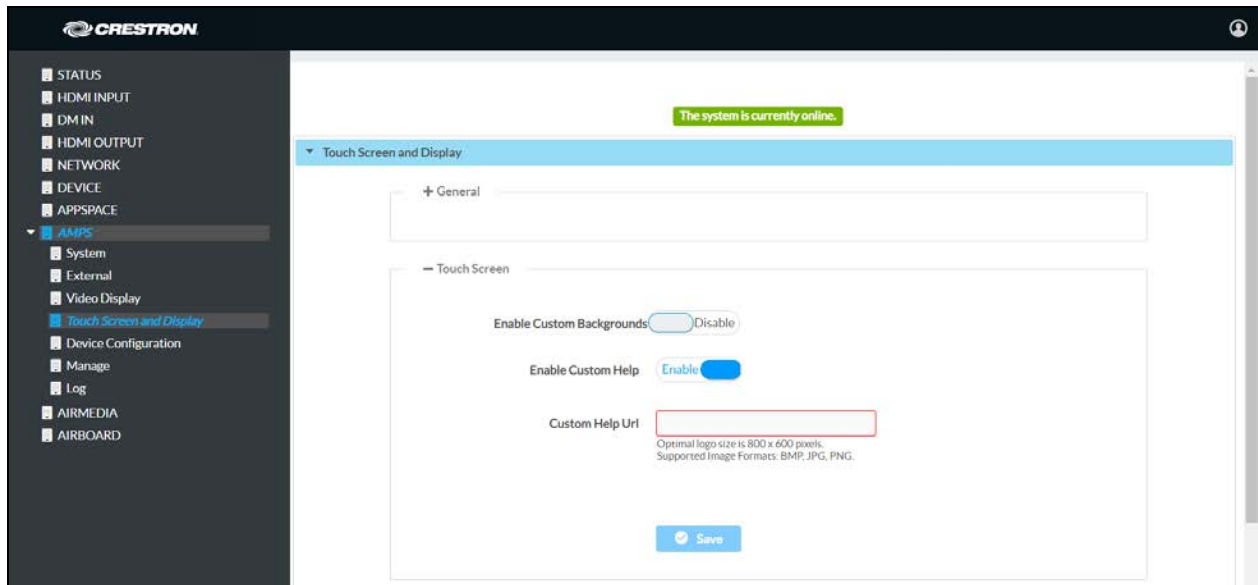
A custom help page image can be shown on the device's connected touch screen when the **Help** button (.AV Framework 1.0 UI) or information button (.AV Framework 2.0 UI) is tapped.

NOTES:

- .AV Framework allocates an area of 800 x 600 pixels for the custom help file graphic. Custom graphics larger than 800 x 600 pixels are not accepted and must be scaled down manually. Custom graphics smaller than 800 x 600 pixels are not scaled up, so these graphics should be resized for optimal image quality.
- Supported custom graphic file types are BMP, JPG, and PNG.

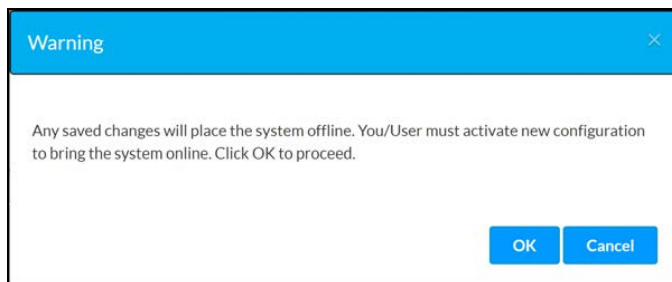
1. Set **Enable Custom Help** to **Enabled**.

AMPS Screen – Touch Screen and Display – Touch Screen



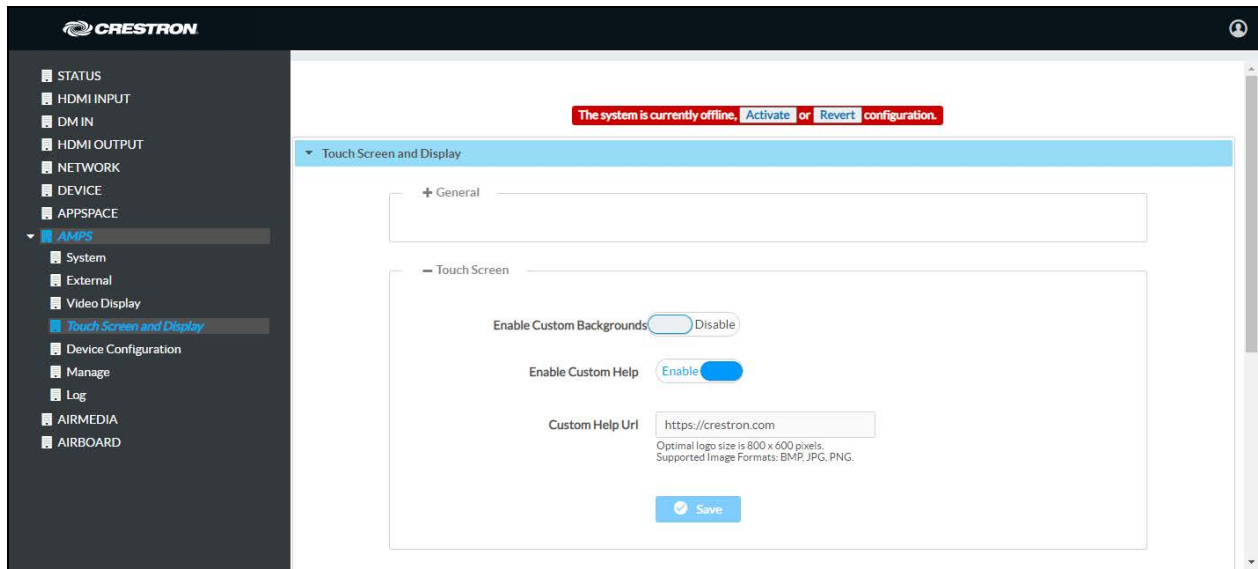
2. Enter the image's location in the **Custom Help URL** field.
3. Click **Save**. A warning message is displayed.

Warning Message



4. Click **OK** to proceed or **Cancel** to cancel.

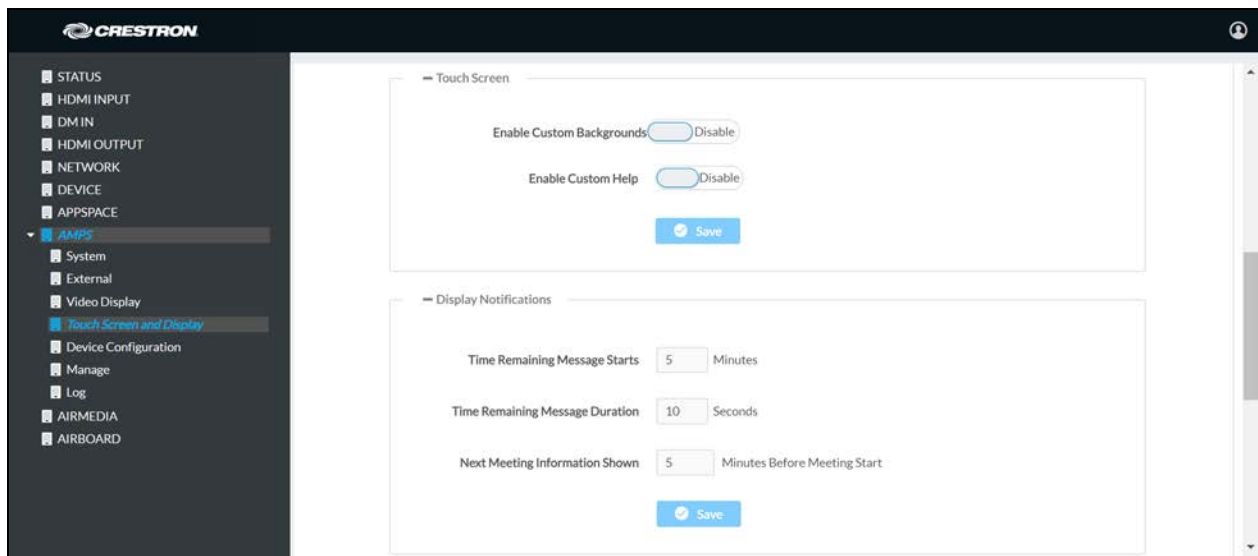
AMPS Screen – Touch Screen and Display – Touch Screen



5. Click **Activate** to activate the new settings and confirm the activation or click **Revert** to undo the changed settings.

Display Notifications

AMPS Screen – Touch Screen and Display – Display Notifications



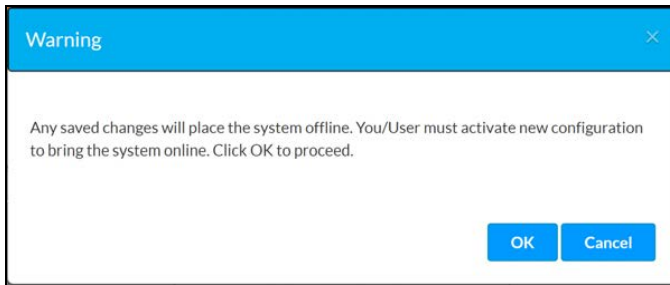
The **Display Notifications** section configures how notifications are displayed while the AM-200 or AM-300 is in use.

1. Configure the following parameters.
 - Enter the amount of time before the meeting's remaining time is displayed in the **Time Remaining Message Starts** field.

- Enter the amount of time the meeting's time remaining message is displayed in the **Time Remaining Message Duration** field.
- Enter the amount of time before the next meeting's information is displayed in the **Next Meeting Information Shown** field.

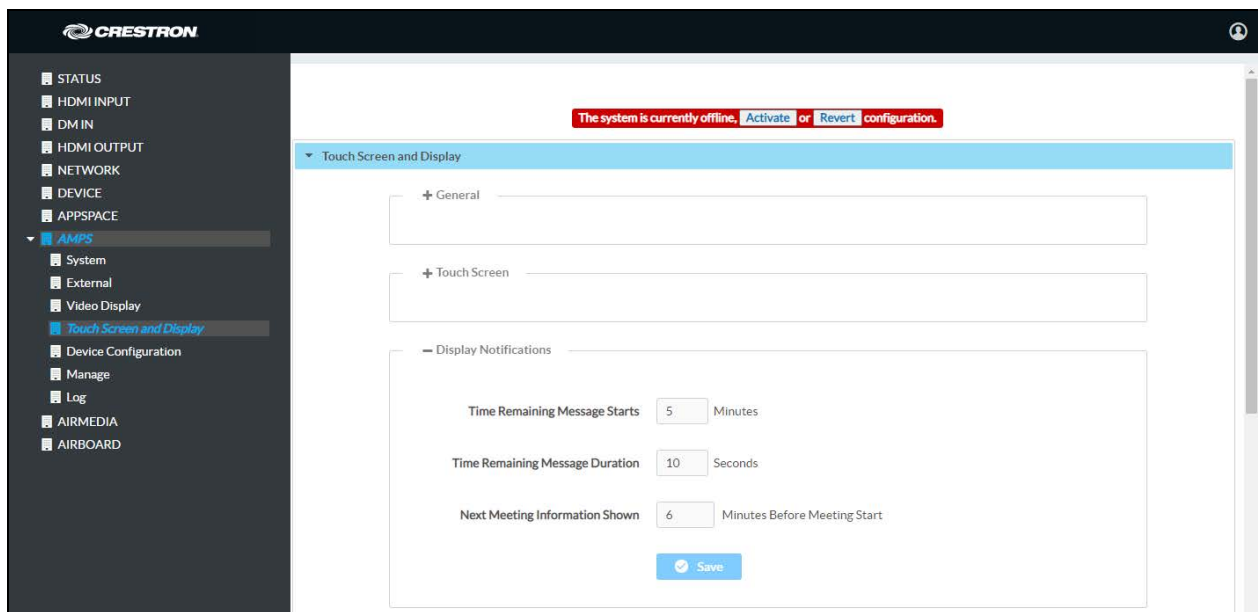
2. Click **Save**. A warning message is displayed.

Warning Message



3. Click **OK** to proceed or **Cancel** to cancel.

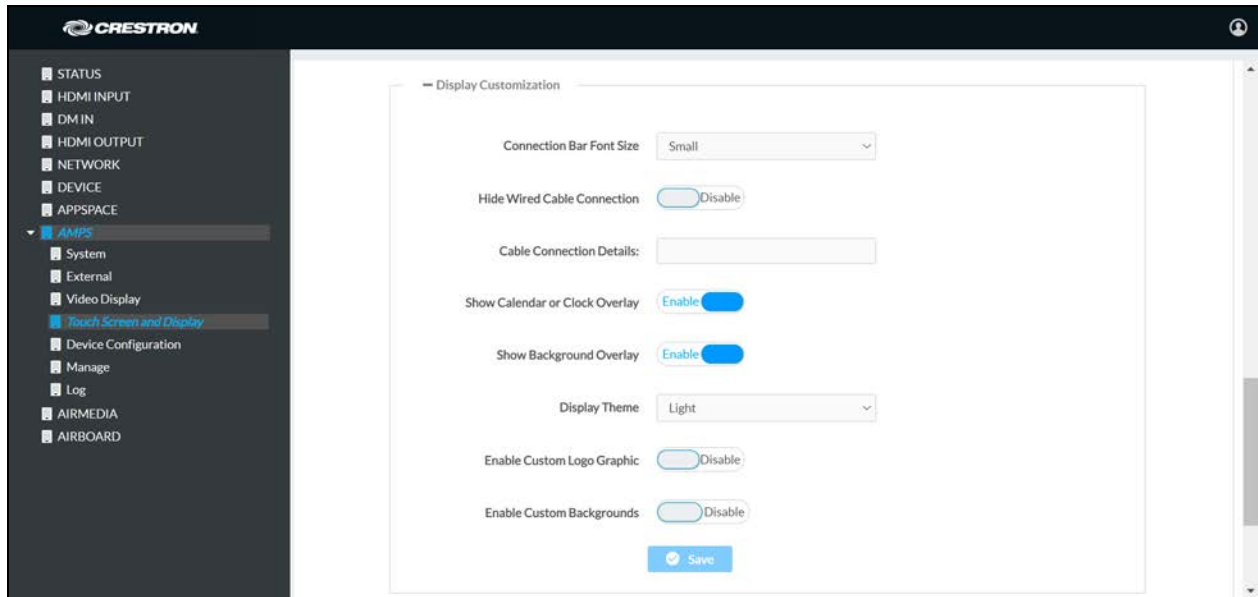
AMPS Screen – Touch Screen and Display – Display Notifications



4. Click **Activate** to activate the new settings and confirm the activation or click **Revert** to undo the changed settings.

Display Customization

AMPS Screen – Touch Screen and Display – Display Customization



The **Display Customization** section configures what is shown on the display device when not in use.

Configure Settings

Make changes to the settings for font size, cable connection details, calendar or clock overlay, background overlay, display theme, custom logo, and custom background.

Font Size

Select the font size of the text (**Small**, **Medium** or **Large**) within the connection bar on the AirMedia Welcome Screen from the **Connection Bar Font Size** drop-down list. When set to **Large**, AirBoard connection information (if configured for use) will be unavailable.

Show Cable Connection Details

Set **Hide Wired Cable Connection** to **Disable** and enter information in the **Cable Connection Details** field to display instructions for using cable connections. The maximum length is 22 characters. To hide information on cable connections, set **Hide Wired Cable Connection** to **Enable**.

Calendar or Clock Overlay

Set **Show Calendar or Clock Overlay** to **Enable** to show the clock and calendared events in the center of the display device. Set **Show Calendar or Clock Overlay** to **Disable** to remove the clock and calendared events from the center of the display device.

Background Overlay

Set **Show Background Overlay** to **Enable** to place a monochrome filter over background images. Set **Show Background Overlay** to **Disable** to remove the filter and show background images in full color.

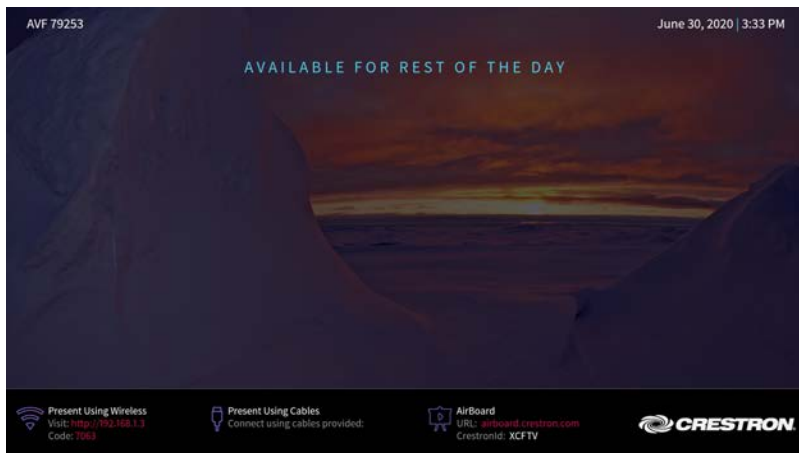
Display Theme

Set **Display Theme** to **Light** to use a light color scheme on the display device or set **Display Theme** to **Dark** to use a dark color scheme on the display device.

Light Color Scheme



Dark Color Scheme



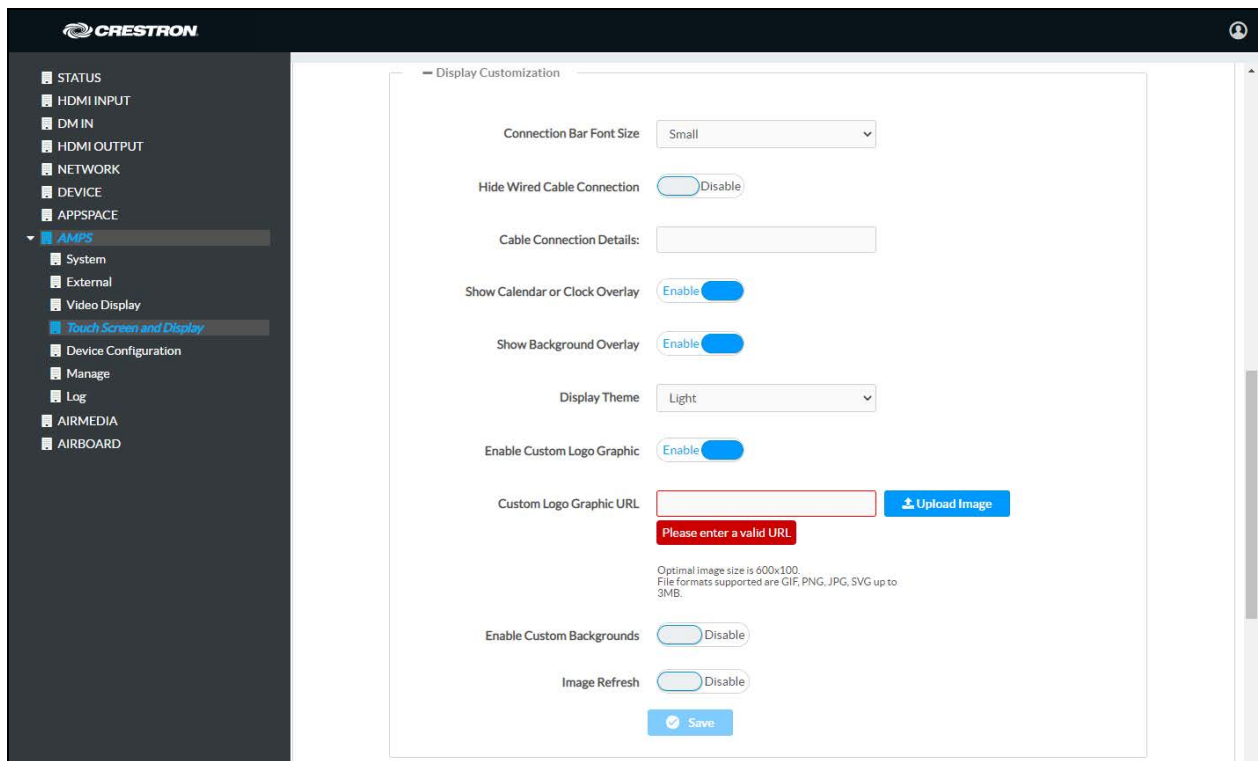
Custom Logo

A custom logo can be displayed in the lower right corner of the display device when the system is not in use. Logo files can be placed on a server or uploaded to the device.

NOTE: The optimal image size for a logo is 480 x 94 pixels. Custom graphics that are larger than 480 x 94 pixels are scaled down while maintaining their aspect ratio. Custom graphics that are smaller than 480 x 94 pixels are not scaled up and should be resized for optimal image display.

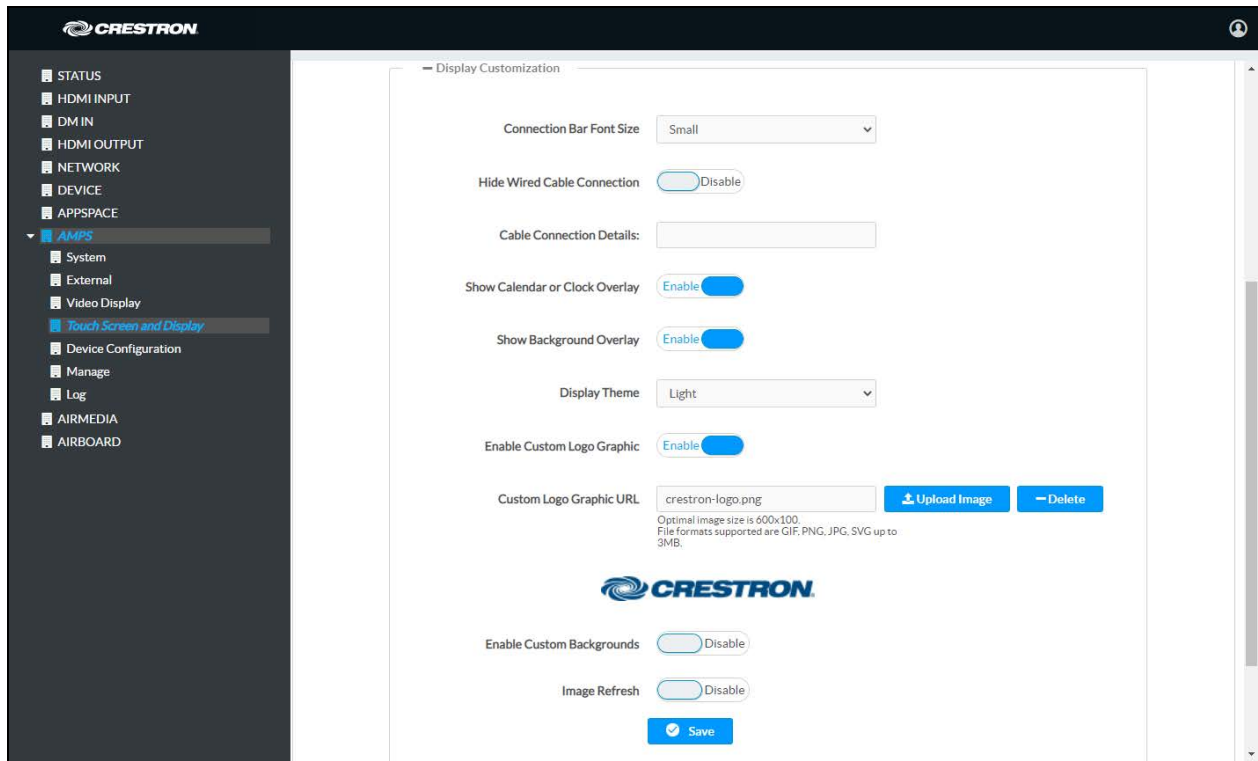
1. Set **Enable Custom Logo Graphic** to **Enable**. When set to **Disable**, the Crestron logo is used.

AMPS Screen – Touch Screen and Display – Display Customization



2. Choose an image on a server or upload a custom image.
 - **Choose an image on a server**
Enter the URL where the image is located in the **Custom Logo Graphic URL** field.
 - **Upload an image**
 - a. Click **Upload Image**.
 - b. Navigate to the location of the image file.
 - c. Select the file and click **Open**.

AMPS Screen – Touch Screen and Display – Display Customization



To delete the logo, click **Delete**.

Custom Backgrounds

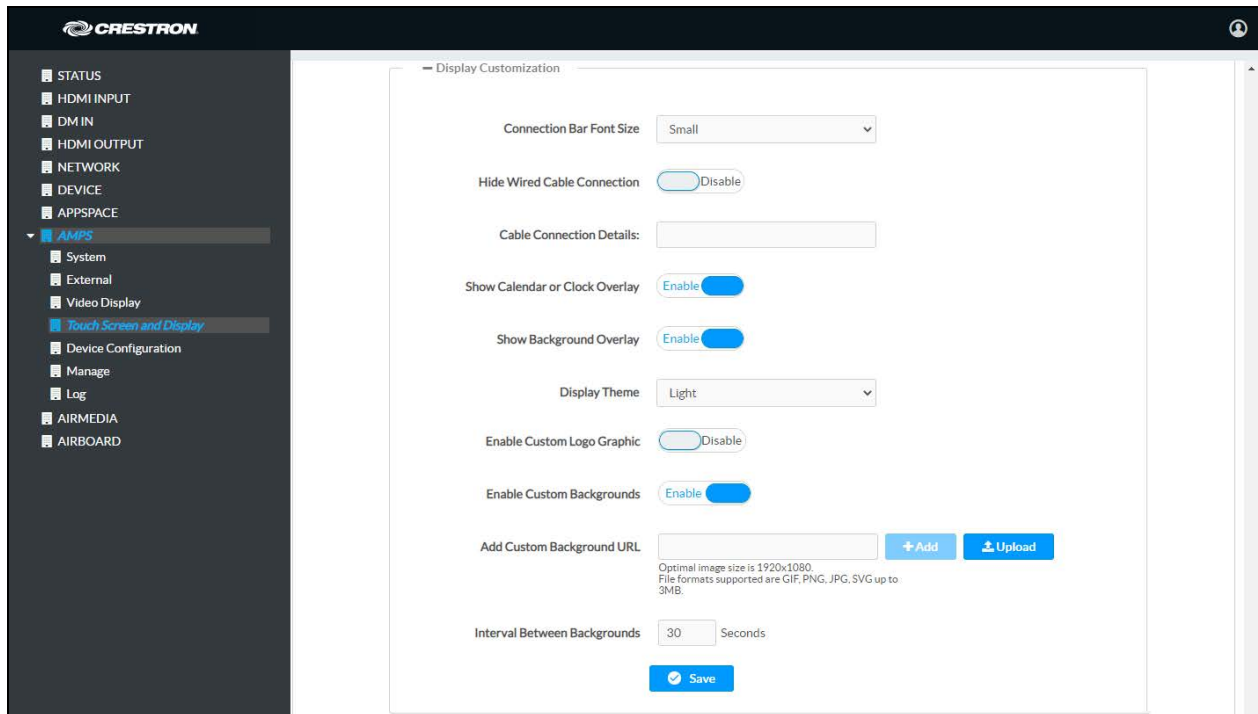
A slideshow of custom backgrounds can be shown on the display device when the system is not in use.

NOTES:

- When Appspace is enabled, custom backgrounds cannot be used. For information on using Appspace, refer to [APPSPACE \(on page 44\)](#).
- 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.

1. Set **Enable Custom Backgrounds** to **Enable**.

AMPS Screen – Touch Screen and Display – Display Customization



2. Choose an image on a server or upload a custom image.

- **Choose an image on a server**

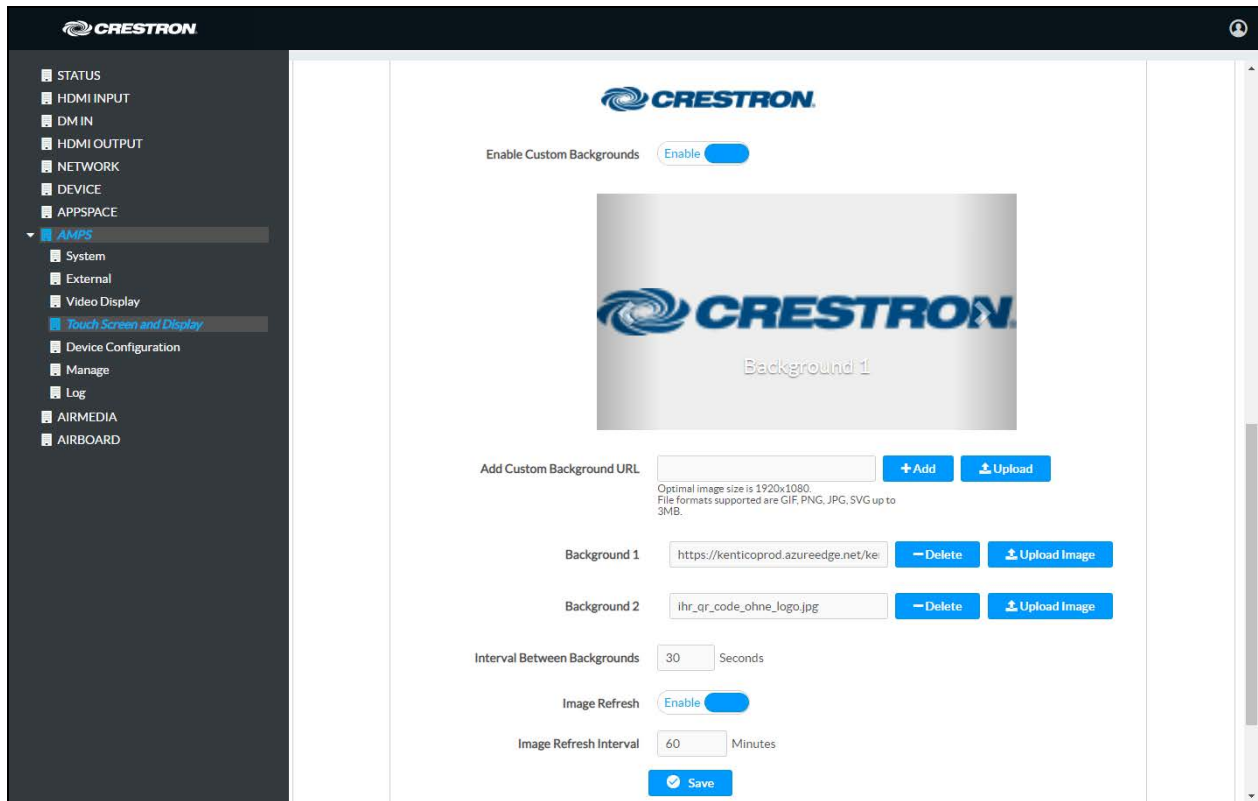
- a. Enter the URL where the image is located in the **Add Custom Background URL** field.
- b. Click **Add**. The image is added to the list of images.

- **Upload an image**

NOTE: Up to 15 images can be stored locally on the device at a maximum of 3 MB.

- a. Click **Upload Image**.
- b. Navigate to the location of the image file.
- c. Select the file and click **Open**. The image is added to the list of images.

AMPS Screen – Touch Screen and Display – Display Customization



3. Repeat step 2 for each background image to be added.
4. Specify the length of time that each background image is displayed, enter a time (in seconds) in the **Interval Between Backgrounds** field.

To delete an image from the slideshow, click the **Delete** button of the image to be deleted.

Image Update

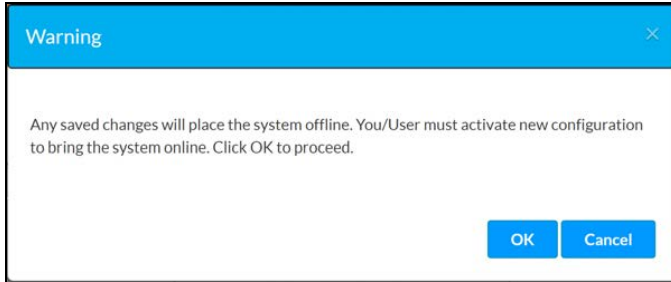
The AM-200/AM-300 can be configured to regularly download the latest versions of remotely stored logo and background image files.

1. Set **Image Refresh** to **Enable** to allow the system to periodically download the remotely stored logo and background images from the URLs specified in the **Custom Logo Graphic URL** and **Add Custom Background URL** fields.
2. Enter the amount of time between downloads (in minutes) in the **Image Refresh Interval** field. The minimum amount of time available is one minute, and the maximum amount of time is 65,535 minutes (about 45 days).

Save Settings

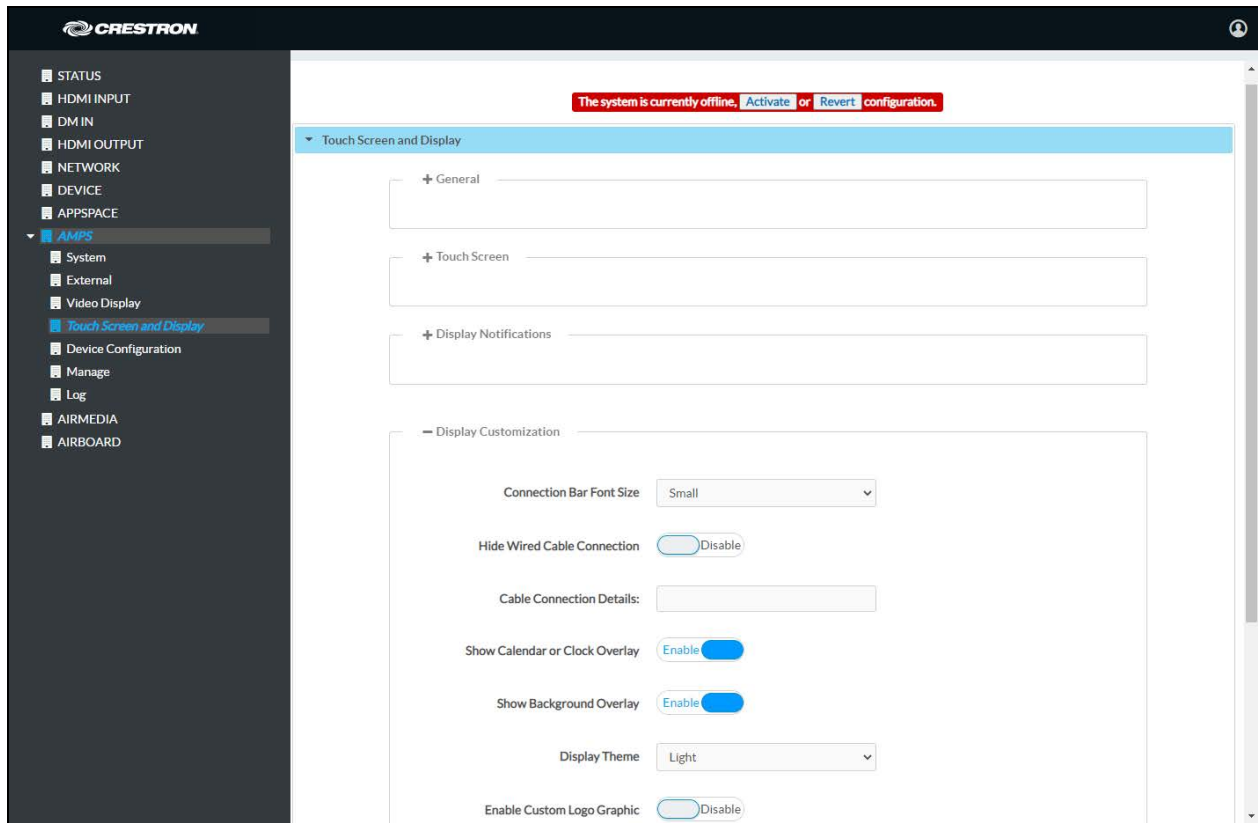
1. Click **Save**. A warning message is displayed.

Warning Message



2. Click **OK** to proceed or **Cancel** to cancel.

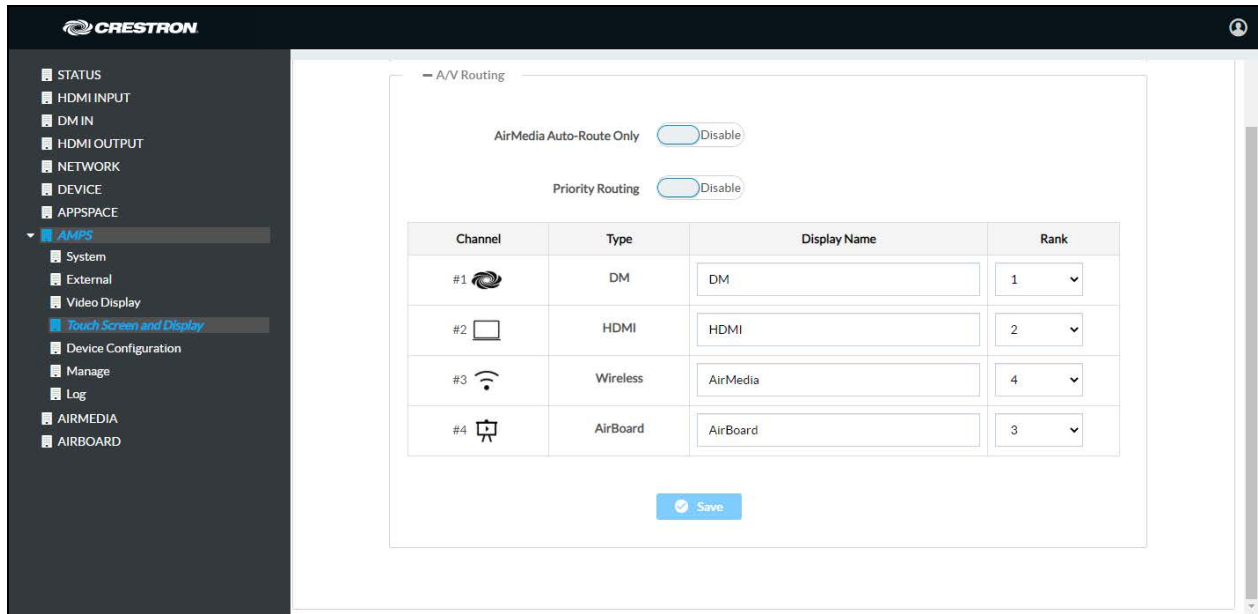
AMPS Screen – Touch Screen and Display – Display Customization



3. Click **Activate** to activate the new settings and confirm the activation or click **Revert** to undo the changed settings.

A/V Routing

AMPS Screen – Touch Screen and Display – A/V Routing



The **A/V Routing** section configures the order in which devices are routed to the display device upon connection. By default, routing is automatic, meaning the last connected source will be routed to the display device.

1. Configure the following parameters.

- Set **AirMedia Auto-Route Only** to **Enable** to have the AM-200/AM-300 automatically route a connected AirMedia source to the display device. Any other sources (DM, HDMI, and AirBoard) must be manually routed from the touch screen. To automatically route any source to the display device when connected, set **AirMedia Auto-Route Only** to **Disable**.
- Set **Priority Routing** to **Enable** to dictate the order in which sources are routed using the chart.

NOTE: **AirMedia Auto-Route Only** must be set to **Disable**.

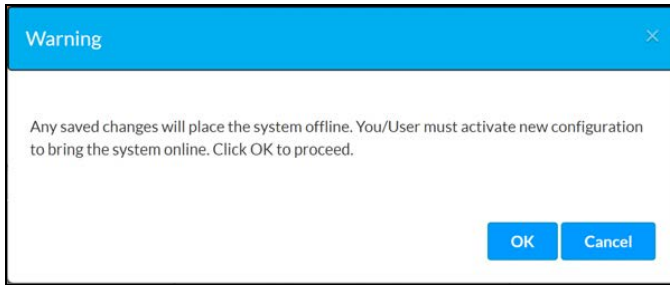
- To change the name of the source that appears on the touch screen, type a name into the text field in the corresponding row of the device.

NOTE: The name may be changed regardless of the **AirMedia Auto-Route Only** setting.

- To change the routing order of a device, select a number from the corresponding drop-down list under the **Rank** column. Devices with a lower number rank will take priority over others.

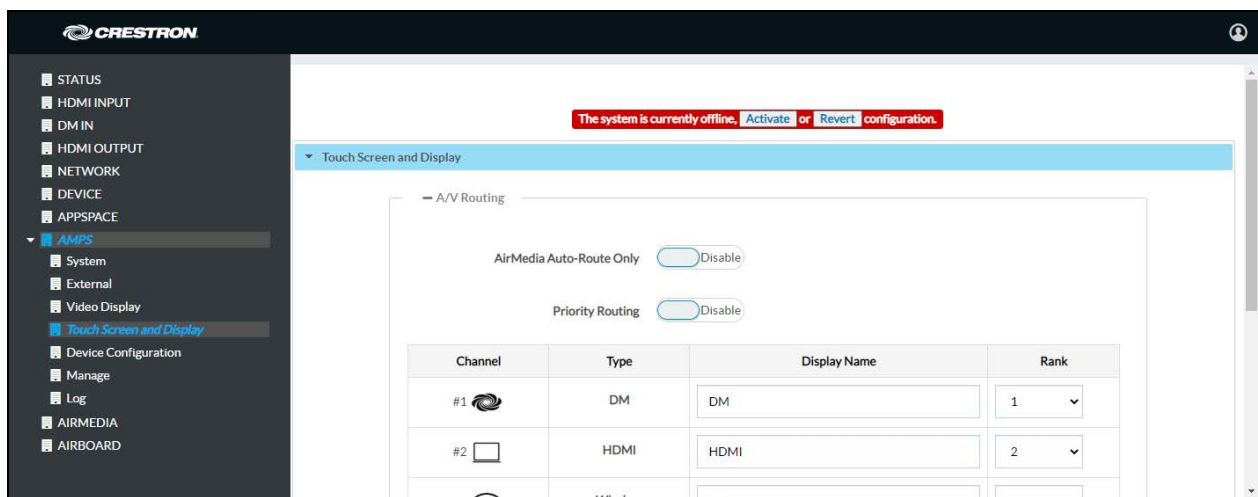
2. Click **Save**. A warning message is displayed.

Warning Message



3. Click **OK** to proceed or **Cancel** to cancel.

AMPS Screen – Touch Screen and Display – A/V Routing



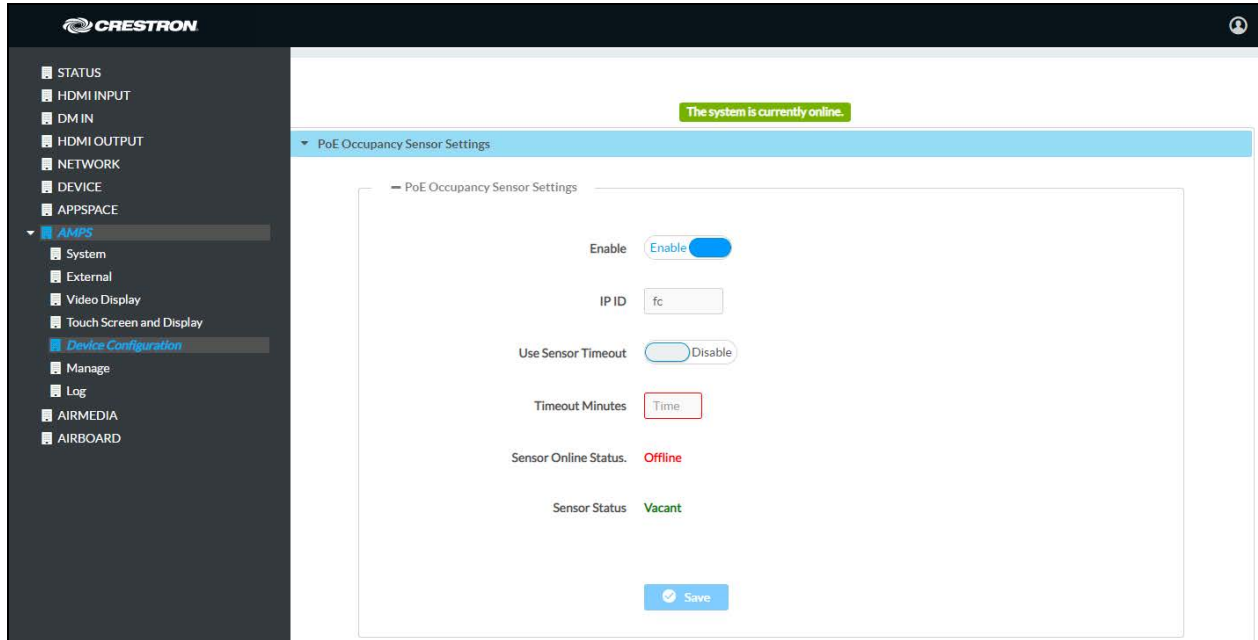
4. Click **Activate** to activate the new settings and confirm the activation or click **Revert** to undo the changed settings.

Device Configuration

PoE Occupancy Sensor Settings

The AM-200 and AM-300 can use the Crestron CEN-ODT-C-POE occupancy sensor for system control based on occupancy, vacancy, and/or business hours. The **PoE Occupancy Sensor Settings** screen is used to enable or disable the occupancy sensor, modify the sensor timeout settings, and check the sensor status.

AMPS Screen – PoE Occupancy Sensor Settings

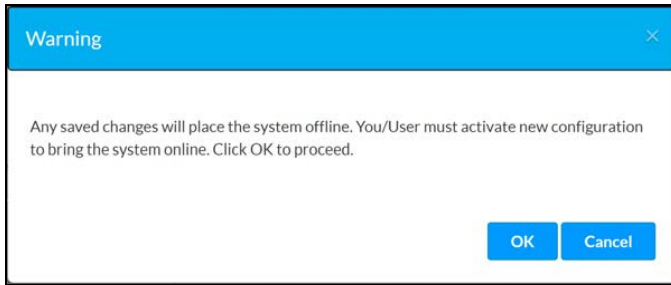


1. Configure the PoE occupancy sensor settings.

- Set **Enable** to **Enable** to use the occupancy sensor with an AM-200 or AM-300. To disable the sensor, set **Enable** to **Disable**.
- In the **IP ID** field, enter the IP ID used by the sensor.
- The system can use a vacant signal from the sensor to change its status, or it can delay the status change after receiving the vacant signal from the occupancy sensor.
 - Set **Use Sensor Timeout** to **Enable** to change the system status when a vacant signal is received from the sensor.
 - Set **Use Sensor Timeout** to **Disable** and enter a timeout period (in minutes) in the **Timeout Minutes** field. The system will change its status when a vacant signal is received from the sensor and the timeout period has passed.
- **Sensor Online Status** indicates whether the sensor is **Online** or **Offline**.
- **Sensor Status** will display whether the room is **Occupied** or **Vacant** based on its reading.

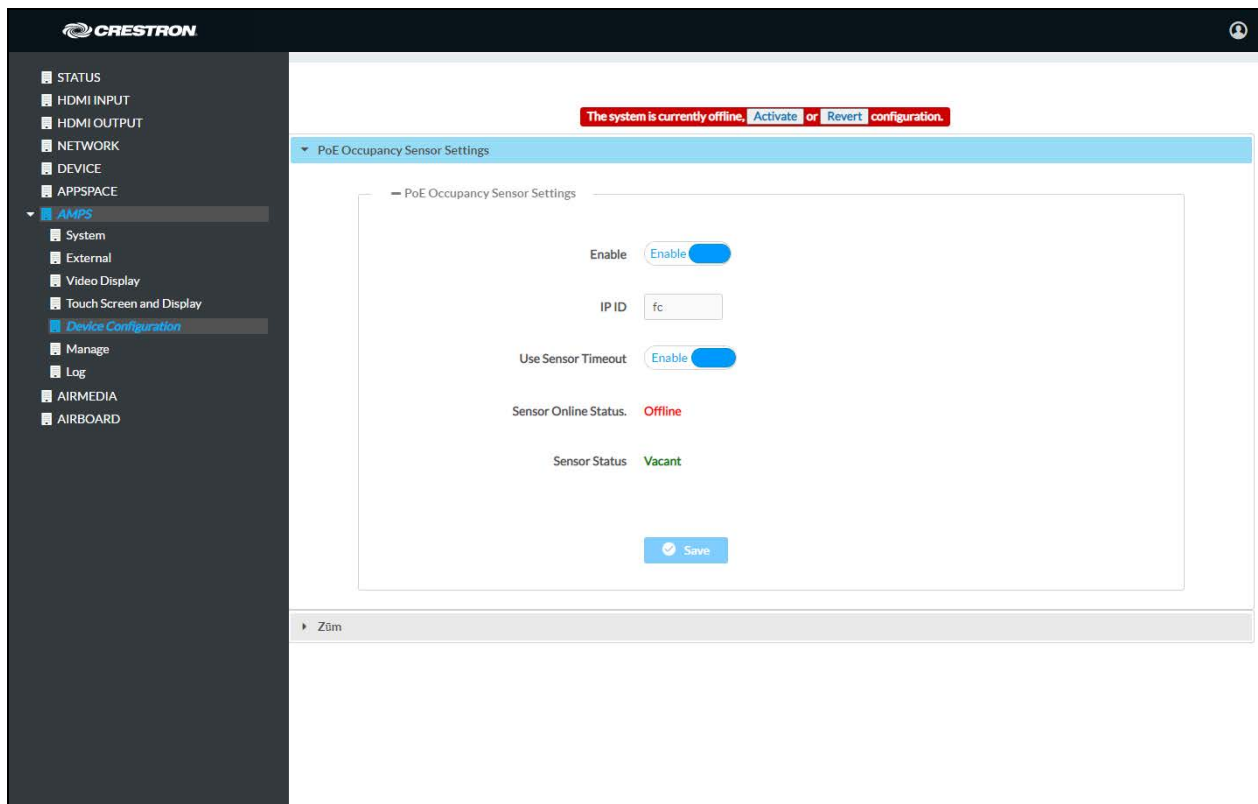
2. When all changes have been made, click **Save**. A warning message is displayed.

Warning Message



3. Click **OK** to proceed or **Cancel** to cancel.

AMPS Screen – Device Configuration – PoE Occupancy Sensor Settings

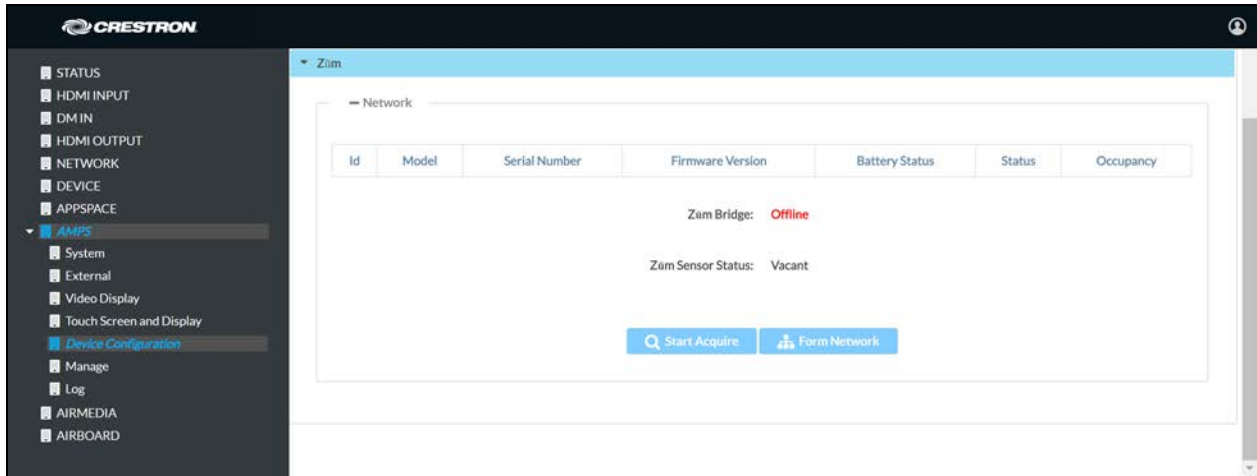


4. Click **Activate** to activate the new settings and confirm the activation or click **Revert** to undo the changed settings.

Zūm

The AM-200 and AM-300 can use Zūm® wireless occupancy sensors and keypads for operation. The **Zūm** screen is used to create Zūm networks, add Zūm devices, and monitor Zūm devices.

AMPS Screen – Zūm



Network

The **Network** section shows all the Zūm devices in the Zūm wireless network.

The **Zūm Bridge** field indicates the status of the connected ZUMMESH-AVBRIDGE or ZUMMESH-AVBRIDGE-I Wireless Control Integration Module.

The **Zūm Sensor Status** field indicates the status of the ZUMMESH-PIR-OCCUPANCY-BATT Wireless Battery-Powered Occupancy Sensor.

Form a Network

The **Form Network** function is used whenever a new network needs to be created (i.e., after a ZUMMESH-AVBRIDGE or ZUMMESH-AVBRIDGE-I (hereafter referred to as the ZUMMESH-AVBRIDGE) is connected to the AM-200 or AM-300).

NOTES:

- Forming a network will erase any previously established network and remove any joined devices.
- Zūm devices can be added and managed from ZUMMESH-AVBRIDGE and supported Zūm devices. Refer to [Add a Zūm Device to the Network \(on page 143\)](#).

1. Click **Form Network**. A new network is created with the ZUMMESH-AVBRIDGE as the center of the network. The ZUMMESH-AVBRIDGE also enters the Joining mode.
2. Acquire Zūm devices to the ZUMMESH-AVBRIDGE. For details on specific Zūm devices, refer to [Add a Zūm Device to the Network \(on page 143\)](#).
3. Click **Stop Acquire** after acquiring Zūm devices. The ZUMMESH-AVBRIDGE will exit the Joining mode.

NOTE: The ZUMMESH-AVBRIDGE will automatically exit the Joining mode after four minutes.

Add a Zūm Device

Supported Zūm devices can be added to an existing network. For a list of supported devices, refer to [Supported Devices \(on page 143\)](#).

1. Click **Start Acquire**. The ZUMMESH-AVBRIDGE enters the Joining mode.
2. Acquire Zūm devices to the ZUMMESH-AVBRIDGE. For details on specific Zūm devices, refer to [Add a Zūm Device to the Network \(on page 143\)](#).
3. Click **Stop Acquire** after acquiring Zūm devices. The ZUMMESH-AVBRIDGE will exit the Joining mode.

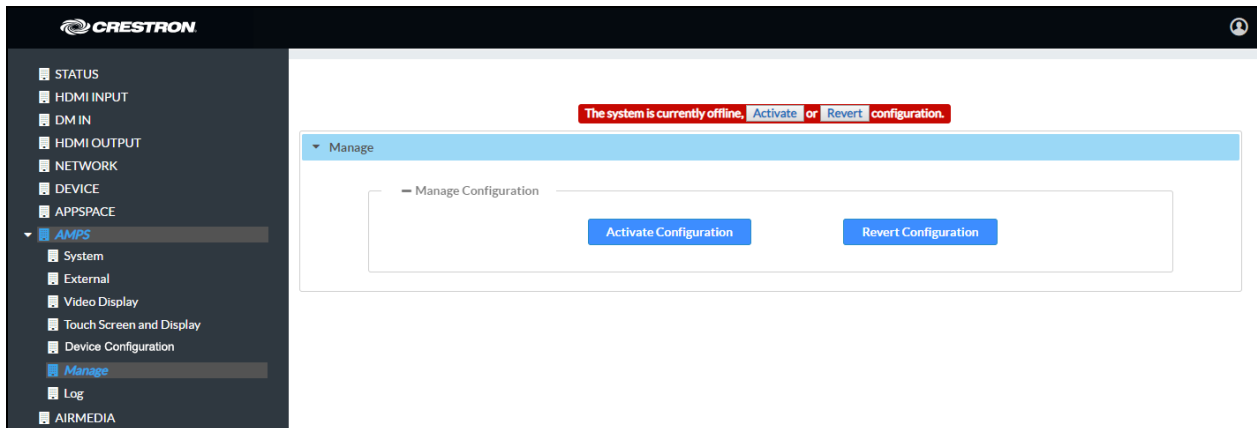
NOTE: The ZUMMESH-AVBRIDGE will automatically exit the Joining mode after four minutes.

Manage

The **Manage** screen is used to enact the changes made in the AMPS menu or to revert to the previous settings.

When changes are made to the AMPS settings, the device goes offline and the screen below is shown.

AMPS Screen – Manage – System Offline



The display device shows a message indicating that the system is currently offline.

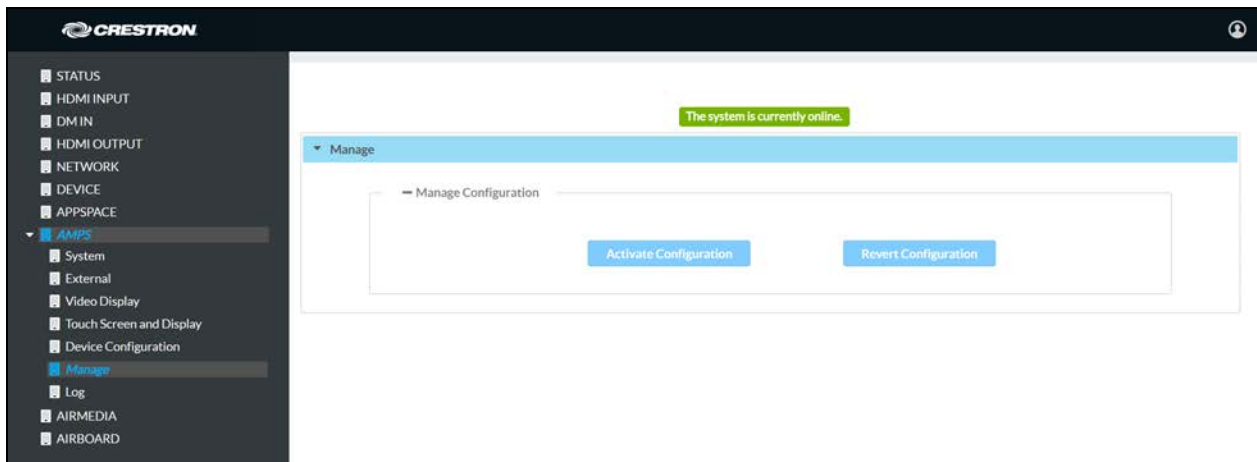
If a touch screen is connected, the following message is shown.

Touch Screen – System Configuration in Progress



Click **Activate** or **Activate Configuration** to carry out the changes that were made, or click **Revert** or **Revert Configuration** to revert back to the previously saved settings. The screen below is shown after activation or reverting to the previously saved settings.

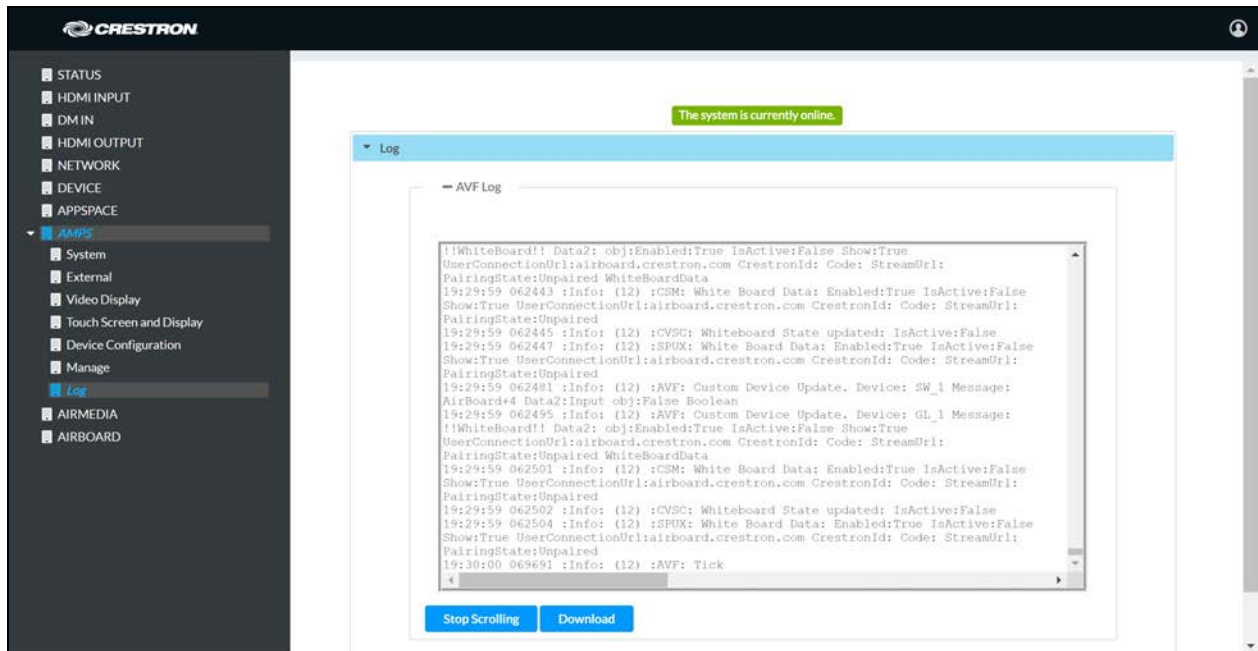
AMPS Screen – Manage – System Online



Log

The **Log** screen is used to view and download the device's message logs for analysis.

AMPS Screen – Log



- Click the up or down arrows to scroll through the message log.
- Click **Stop Scrolling** to pause the message log. Click **Scrolling** to resume.
- Click **Download** to download the message log.

AirMedia

Click **AIRMEDIA** to configure the device's AirMedia functionality. The **AIRMEDIA** screen is displayed.

AIRMEDIA Screen

The screenshot displays the Crestron AirMedia configuration interface. On the left is a navigation menu with options: STATUS, HDMI INPUT, DM IN, HDMI OUTPUT, NETWORK, DEVICE, APPSPACE, AMP5, AIRMEDIA (selected), and AIRBOARD. The main content area is titled 'AirMedia' and contains several sections:

- AirMedia:** Includes toggle switches for AirMedia (Enabled), AirMedia Certificate (Disabled), Force Secure Landing Page (HTTPS) (Disabled), AirMedia Discovery (Enabled), and Air Media Canvas (Enabled). A note states: "Note: Canvas cannot be disabled if the Air Media Connection Overlay is enabled." Canvas Options are set to "All Sources Types".
- Code:** Login Code Mode is set to "Random". Login Code is "8881" with a "Set" button. Display Login Code is Enabled.
- Ethernet Adapter:** Assigned Ethernet Port is set to "LAN" and "WLAN".
- Connection Display Options:**
 - General:** Show AirMedia Connection Info Overlay is Disabled. Note: "When AirMedia Connection Overlay is enabled, Canvas cannot be disabled."
 - LAN Connection Information:** Show Connection Info is Enabled. Connection Info Mode is "IP Address". Custom String is empty.
 - Wi-Fi Connection Information:** Show Wi-Fi Connection SSID is Enabled. SSID Options are "Custom" (SSID: "test2"). Key Options are "Custom" (Key: "test"). Show Connection Info is Enabled. Connection Info Mode is "IP Address". Custom String is empty.
- Miracast:** Miracast is Disabled. Default Windows Experience is "Miracast". Wi-Fi Dongle Status is "Connected". Miracast Connection Modes include "Wi-Fi Direct Mode" (Enabled) and "Infrastructure Mode" (Enabled). A note states: "▲Wi-Fi Direct Mode requires that Login Code be set to Random or Fixed. Miracast connection requires that one or both of the 'Wi-Fi Direct Mode' and 'Infrastructure Mode' parameters be enabled."
- AirMedia Application Downloads:** Windows Application Download is set to "Cloud Download" with an "Update Now" button. Server URL is empty. MacOS Application Download is also set to "Cloud Download" with an "Update Now" button. Server URL is empty.

At the bottom, there is a copyright notice: "© 2020 Crestron Electronics, Inc." and a link to the "Privacy Statement | Crestron Unified Communication Software License Agreement".

AirMedia can support up to 10 simultaneously connected AirMedia application users (Windows or Android operating systems) and a maximum of 2 native mirroring users (Airplay/Miracast) of which, two sources can present to the display simultaneously using the AirMedia Canvas feature. For details on the AirMedia canvas feature, refer to [AirMedia Canvas \(below\)](#).

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

AirMedia

Set **AirMedia** to **Enabled** to enable wireless presentation using AirMedia technology. To turn off AirMedia, set **AirMedia** to **Disabled**.

AirMedia Certificate

The AirMedia receiver within the AM-200 and AM-300 supports third party certificates for encrypting connections between the sender applications for Windows and Android and the receiver.

1. Set **AirMedia Certificate** to **Enabled** to use a third party certificate. The AM-200/AM-300 must be rebooted.
2. Load a certificate onto the device as described in [Certificate Authentication \(on page 24\)](#).

Force to a Secure Landing Page

The AM-200 and AM-300 can force connecting devices to a secure landing page (HTTPS).

Set the **Force Secure Landing Page (HTTPS)** setting to **Enabled**. When enabled, the web server uses either the certificate loaded in the certificate store (when available) or a self-signed certificate. When this setting is enabled, the AirMedia connection URL will contain HTTPS.

AirMedia Discovery

By default, the AM-200 and AM-300 are configured for automatic discovery by the AirMedia application. To prevent the AM-200 and AM-300 from discovery by the AirMedia application, set **AirMedia Discovery** to **Disabled**. Users who wish to use the AirMedia application with the device will be required to manually enter the IP address or host name of the AM-200/AM-300.

AirMedia Canvas

The AM-200 and AM-300 can be configured to have two sources present simultaneously on the display using the AirMedia Canvas feature. AirMedia Canvas automatically configures the best possible layout to maximize screen coverage based on the number of sources active, 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 or DM

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.

- Crestron AirBoard Whiteboard Capture System

Set the **Canvas** setting to **Enabled** to enable the AirMedia Canvas feature. Once enabled, select one of the following options:

- Select **All Sources Types** to allow all source types (DM, HDMI, AirMedia, and Crestron AirBoard Whiteboard Capture System) to be share space on the display.
- Select **Network Source Types Only** to allow only wireless sources (AirMedia, Miracast, AirPlay and Crestron AirBoard Whiteboard Capture System) to share space on the display. HDMI and DM sources will present in full screen if selected.

NOTE: The AirMedia Canvas feature cannot be disabled when the AirMedia Connection Overlay feature is enabled. For details on the AirMedia Connection Overlay feature, refer to [General \(on the facing page\)](#).

When enabled, AirMedia Canvas works as follows:

- If one source is active, the source shall be presented in full screen.
- If two sources are active, the sources shall be presented side-by-side in a configuration that maximizes the screen coverage depending on the aspect ratio of the sources.
- When two sources are active, and one of the two sources is disconnected, the single source shall return to full screen.
- If a third source is active, the first active source is stopped (AirMedia user) or disconnected (hard wired inputs, AirPlay connection, or Miracast connection).
- When all sources are disconnected, the display will show the front of the room experience splash screen.

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

Source switching and layout can also be managed by a touch screen that is using the .AV Framework 2.0 theme. For details on using a touch screen to control AirMedia canvas, refer to [AirMedia Canvas \(on page 123\)](#).

NOTE: The touch screen must be set to use the .AV Framework 2.0 user interface theme to control AirMedia Canvas. For details on setting the theme, refer to [General \(on page 71\)](#).

Code

A code can be used to limit access to the device. The code feature can be disabled, randomly generated, or fixed to a specific value. Select one of the following Login Code Modes 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** sets the device to randomly generate 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.
- **Use the following code** sets the device to display a user-specified, four-digit access code.
 1. Enter a code in the **Login Code** field.
 2. Click **Set**. The access code will be shown on the display device when the **Display Login Code** setting is set to **Enabled**.
- Set **Display Login Code** to **Enabled** to show the access code on the display device. Set **Display Login Code** to **Disabled** to hide the login code.

Ethernet Adapter

Select the Ethernet ports assigned for use by AirMedia.

- Select **LAN** to allow AirMedia connections from the local area network.
- Select **WLAN** to allow AirMedia connections from the AM-200/AM-300's self hosted Wi-Fi access point.

NOTE: The [AM-USB-WIFI](#) or [AM-USB-WF](#) AirMedia USB Adapter with Wi-Fi Connectivity (sold separately) is required. For details on configuring the Wi-Fi access point, refer to [Wireless Configuration \(on page 30\)](#).

Connection Display Options

Select whether connection information is shown on the display device as well as what connection information is displayed.

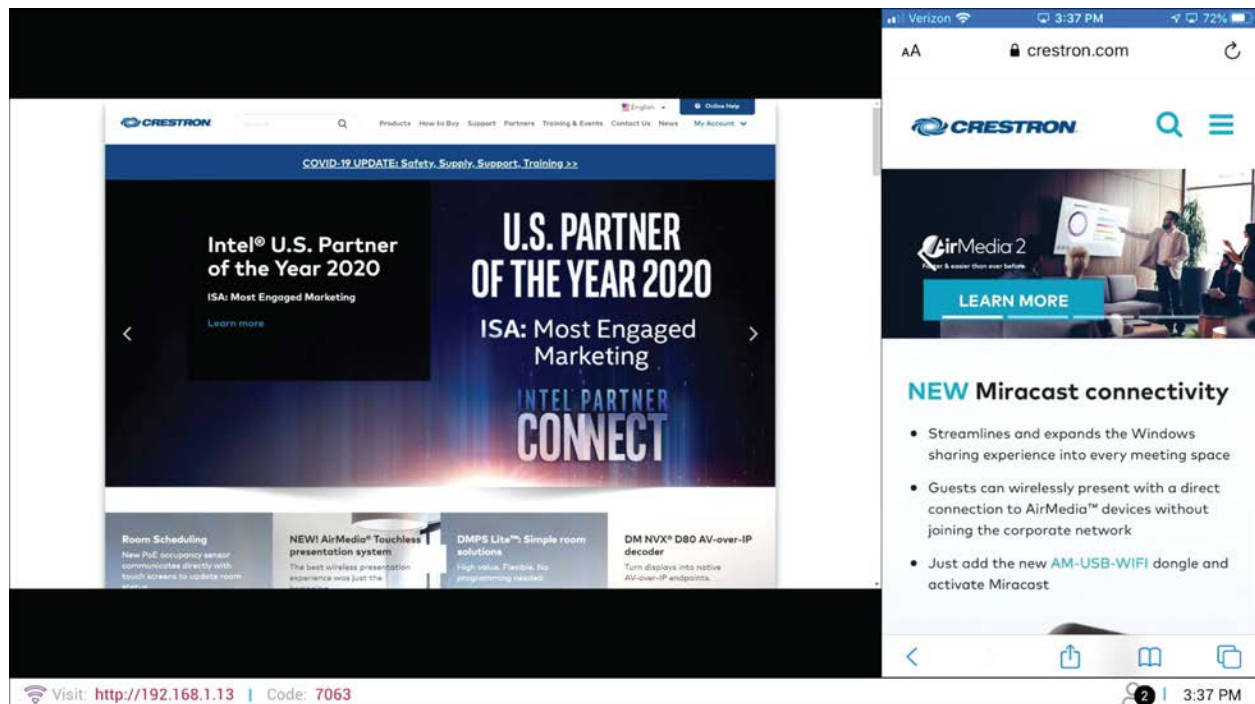
General

If the AirMedia Canvas feature is enabled, you can select whether AirMedia connection details are shown on the display device while a source is presenting.

Set **Show AirMedia Connection Info Overlay** to **Enabled** to show connection information. Otherwise, set **Show AirMedia Connection Info Overlay** to **Disabled**.

For an optimal user experience, set **Show AirMedia Connection Info Overlay** to **Enabled**.

AirMedia Connection Information Overlay



AirMedia connection information overlay

LAN Connection Information

- Set **Show Connection Info** to **Enabled** to display connection information on the display device. Set **Show Connection Info** to **Disabled** to hide connection information.
- If **Show Connection Info** is set to **Enabled**, select the **Connection Info Mode** to determine what connection information is presented to room visitors.
 - Select **IP Address** to show the IP address to use for connecting to the system.
 - Select **Host** to show the host name to use for connecting to the system.
 - Select **Host And Domain** to show the host name and domain name to use for connecting to the device.
 - Select **Custom** to show a custom string to use for connecting to the system. If a custom string is to be used, enter it in the **Custom String** field.

Wi-Fi Connection Information

The AM-200/AM-300 can be configured to show Wi-Fi connection information on the display device. The AM-200/AM-300 can be set to display the following information:

- **Wi-Fi network name (SSID):** The name of the Wi-Fi access point or the name of a local Wi-Fi network.
- **Security key:** The security key of the Wi-Fi access point or a local Wi-Fi network.

- **Connection Details:** The IP address, host name, host name and domain name, or a custom address for the AirMedia device.

Configure Wi-Fi connection information to be shown on the display device:

- Set **Show Wi-Fi Connection SSID** to **Enabled** to show the name of the Wi-Fi network. Once enabled, the Wi-Fi access point's SSID or the name of the local Wi-Fi network can be shown on the display device.
 - Select **Use WLAN SSID** to use the network name specified when the wireless access point was configured (refer to [Wireless Configuration \(on page 30\)](#)).
 - Select **Custom** and enter the name of the local Wi-Fi network in the **Custom** field.
- Set **Show Wi-Fi Connection Key** to **Enabled** to show the Wi-Fi network's security key. Once enabled, the Wi-Fi access point's security key or the local Wi-Fi network's security key can be shown on the display device.
 - Select **Use WLAN Key** to use the security key specified when the wireless access point was configured (refer to [Wireless Configuration \(on page 30\)](#)).
 - Select **Custom** and enter the local Wi-Fi network's security key in the **Custom** field.
- Set **Show Connection URL** to **Enabled** to show the AirMedia device's Wi-Fi connection details. Once enabled, select whether the device's IP address, host name, host name and domain name, or a custom address are shown on the display device.
 - Select **IP Address** to display the device's IP address.
 - Select **Hostname** to display the device's host name.
 - Select **Host and Domain** to display the device's host name and domain name.
 - Select **Custom** and enter a custom connection string in the **Custom** field.

NOTE: The **Custom** setting is used to display connection information for local wireless infrastructure. If custom naming is to be used, the **SSID Options**, **Key Options**, and **Connection Info Mode** parameters must use the **Custom** setting.

Miracast

Miracast technology allows users to wirelessly share content from a Microsoft® Windows® 10 device via the AM-200/AM-300. Miracast technology is built into the Microsoft Windows 10 operating system, so no additional software installation is required.

NOTES:

- An [AM-USB-WIFI](#) or [AM-USB-WF-I](#) AirMedia Wi-Fi® USB Adapter (sold separately) must be installed on the AM-200/AM-300 to use the Miracast feature. For details, refer to the [AM-USB-WIFI/AM-USB-WIFI-I Quick Start Guide](#) (Doc. 8494).
- When using Miracast, the Zūm AV Bridge is not supported.
- Refer to the [AirMedia Presentation Gateway Deployment 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 such as the AM-200 or AM-300. Once the AM-200 or AM-300 is discovered by the Windows 10 device, it is presented in a list on the device. The user can then select the AM-200 or AM-300 for connection to the Windows 10 device.

During the connection phase, the Windows 10 device will first attempt to connect to the AM-200 or AM-300 through the existing network infrastructure (Infrastructure Mode). If the connection over infrastructure fails, the Windows 10 device will connect to the AM-200 or AM-300 through a Wi-Fi Direct connection to the AM-USB-WIFI AirMedia Wi-Fi Adapter that is installed on the AM-200/AM-300 (Wi-Fi Direct Mode).

NOTE: Miracast operation requires that **Wi-Fi Direct Mode, Infrastructure, or Wi-Fi Direct Mode and Infrastructure** be set to **Enabled**.

1. Set **Miracast** to **Enabled**. A dialog box prompting a reboot will appear. Select **Yes**. The AM-200/AM-300 will reboot.
2. After the reboot procedure is complete, log in and navigate to the **Miracast** section.
3. Set the **Default Windows Experience** to **Miracast** so that instructions for using **Miracast** will appear in the web browser when a user clicks **Start Presenting** on the AirMedia landing page from a Windows device. A dialog box prompting a reboot will appear. Click **Yes** to reboot the AM-200/AM-300.

NOTE: If **AirMedia Windows Sender** is selected as the Default Windows Experience, Windows 10 users will be prompted to download and use the AirMedia sender application to present content instead of using Miracast.

4. Set **Wi-Fi Direct Mode** to **Enabled** so that if the initial connection to the network infrastructure fails, a Wi-Fi point-to-point connection (Wi-Fi Direct®) will occur.
5. Set **Infrastructure Mode** to **Enabled** to connect using the existing network infrastructure (default setting). Otherwise, set **Infrastructure Mode** to **Disabled** to connect using Wi-Fi Direct only.

AirMedia Application Downloads

The administrator can configure where the AM-200 and AM-300 obtain the AirMedia applications that are presented to the user for download as described in [Use AirMedia \(on page 126\)](#). The administrator can specify the version that is included with the device's firmware, the latest version that is in the Cloud, or a version of the application that is hosted on a server.

NOTE: Different settings can be applied for the Windows and MacOS AirMedia applications.

- Select **Off** to use the version of the AirMedia application that is included with the device's firmware.

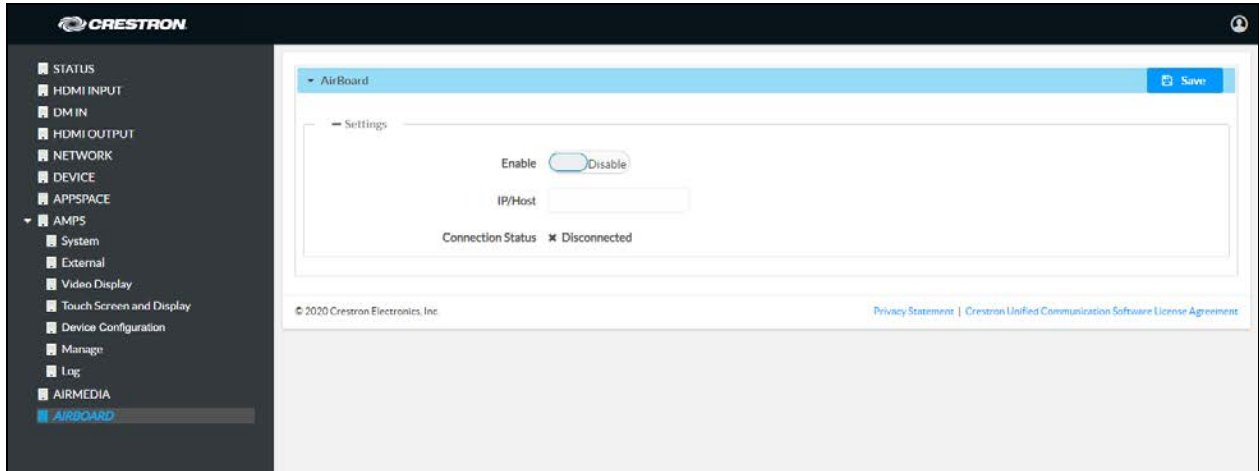
- Select **Cloud Download** to provide Crestron's latest version of the AirMedia application that is stored in the Cloud. The AM-200/AM-300 will check for an update once a day at 2:00 am (local time). Click **Update Now** to update the AirMedia application to the version stored in the Cloud.
- Select **Remote Server** to use a version of the AirMedia application that is hosted on a remote server. Once selected, enter the URL of the remote server in the **Server URL** field. Click **Update Now** to update the AirMedia application to the version hosted on the remote server.

NOTE: If you change the setting from **Cloud Download** or **Remote Server** to **Off**, the AM-200/AM-300 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).

Crestron AirBoard

Click **AIRBOARD** to configure the device's functionality with the Crestron AirBoard™ (CCS-WB-1). The **AIRBOARD** screen is displayed.

AIRBOARD Screen



Settings

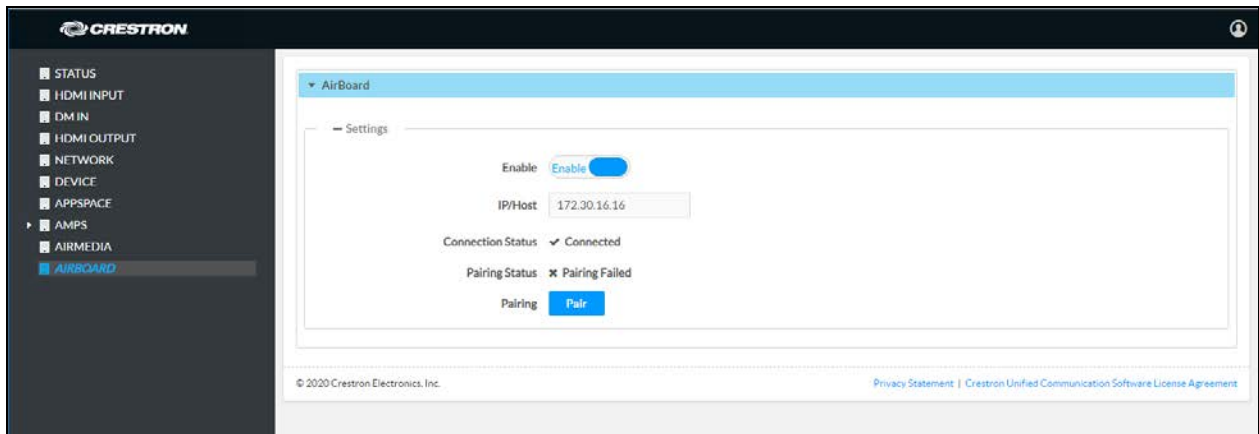
Connect

Connect the Crestron AirBoard to the AM-200/AM-300.

1. Set **Enable** to **Enable**.
2. Enter the Crestron AirBoard's IP address or host name in the **IP/Host** field.
3. Click **Save**.

The Connection Status is displayed below the IP/Host field.

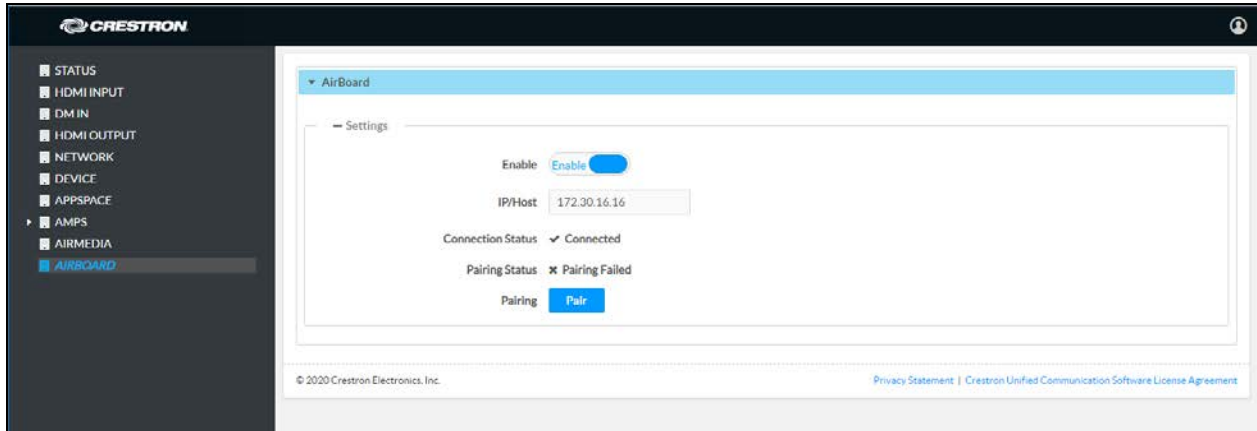
Connection Status



NOTE: After entering the IP address, it may take up to 1 minute for the connection status to update.

Pair the Device

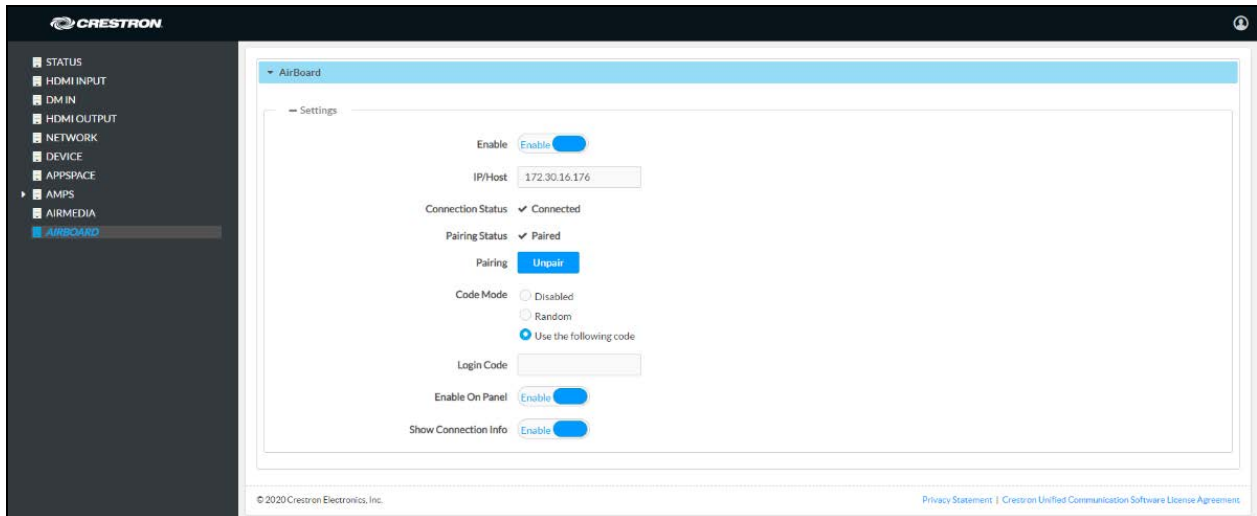
Pair the Device



Once the Crestron AirBoard is connected, it must be paired with the AM-200/AM-300.

1. Click **Pair**.
2. On the Crestron AirBoard's control pad, press the blue button to pair the device. The status will be updated as shown below.

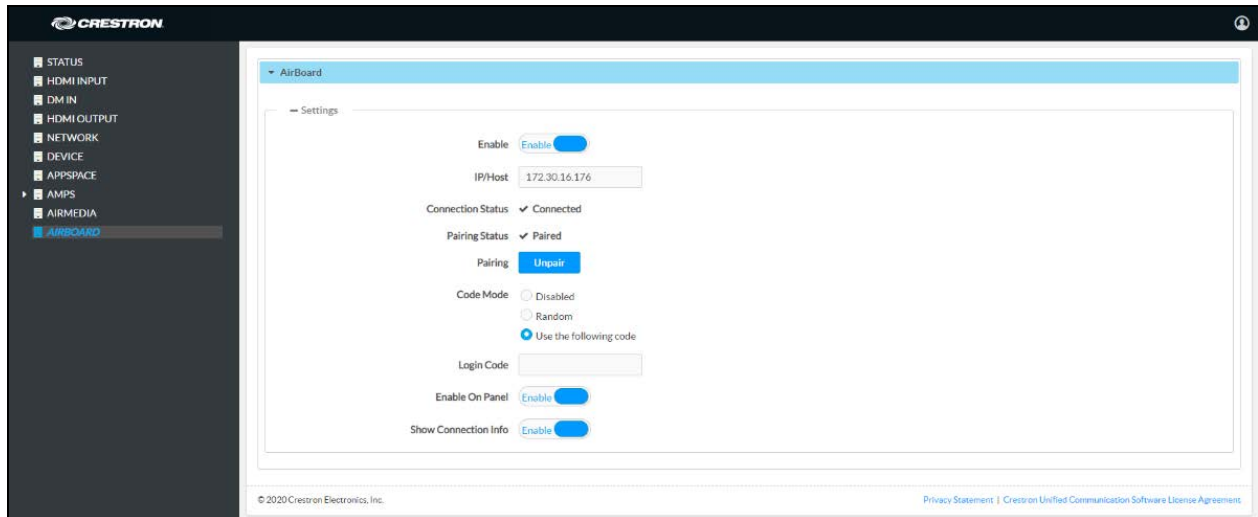
Paired with Crestron AirBoard




Configure for Use

Once the Crestron AirBoard is paired, it can be configured for use.

Configure for Use



1. Select one of the following Code Modes 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** sets the device to randomly generate an access code. A new code is generated when the last connected participant disconnects from the device. The access code is shown on the display device.
 - **Use the following code** sets the device to display a user-specified, four-digit access code. Enter a code in the **Login Code** field.
2. Set **Enable On Panel** to **Enable** to allow Crestron AirBoard presentation as a presentation option on a connected touch screen. When enabled,  will also appear in the touch screen's taskbar. Set **Enable On Panel** to **Disable** to remove Crestron AirBoard from the list of presentation options.
3. Set **Show Connection Info** to **Enable** to display connection information on the display device when no source is active. Set **Show Connection Info** to **Disable** to stop displaying connection information.

To unpair the Crestron AirBoard from the AM-200 or AM-300, click **Unpair**.

Crestron AirBoard Functional Recommendations and Notes:

- Crestron AirBoard functionality requires a TSW touch screen.
- A Crestron AirBoard recording session must be initiated before it can be routed to the display device.
- If the AM-200 or AM-300 is rebooted, the presentation routing to the display device is stopped. However, the active Crestron AirBoard session is not stopped.
- If a Crestron AirBoard device is to be used with another system, it must be unpaired from the original system's web user interface before it can be paired again with another system.
- The Crestron AirBoard device does not distinguish between the organizer and participants. Any allowed participant can accept or invite any other participant into the session. Any participant who knows the login code can join an active session and share a link with the login code to any other person, allowing them to join the session without knowledge of the organizer.

Enterprise Deployment Options

Crestron has two options for deploying multiple AM-200 and AM-300 devices across an enterprise. These tools can assist in deploying any number of AM-200 or AM-300 devices that an organization may need to deploy.

For more information, refer to Answer ID 5719 in the Online Help section of the Crestron website (www.crestron.com/onlinehelp).

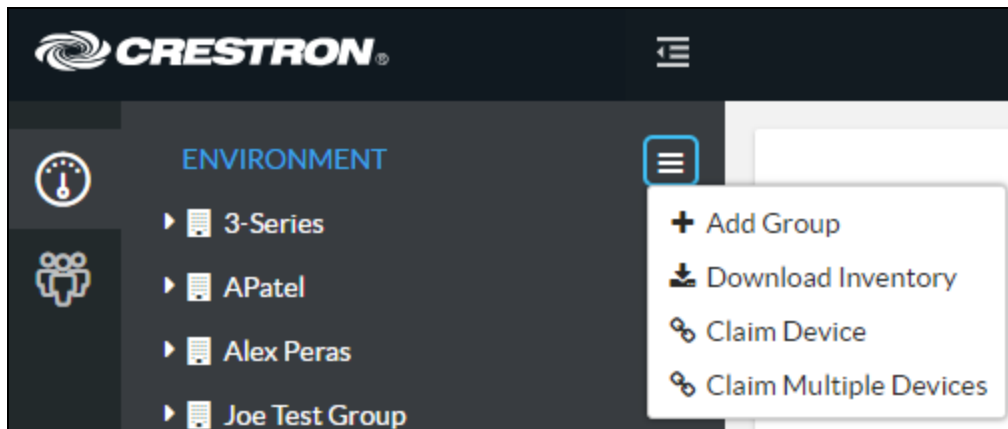
XiO Cloud Service

The XiO Cloud service requires devices to be claimed so they can be managed by the service.

Claim a Single Device

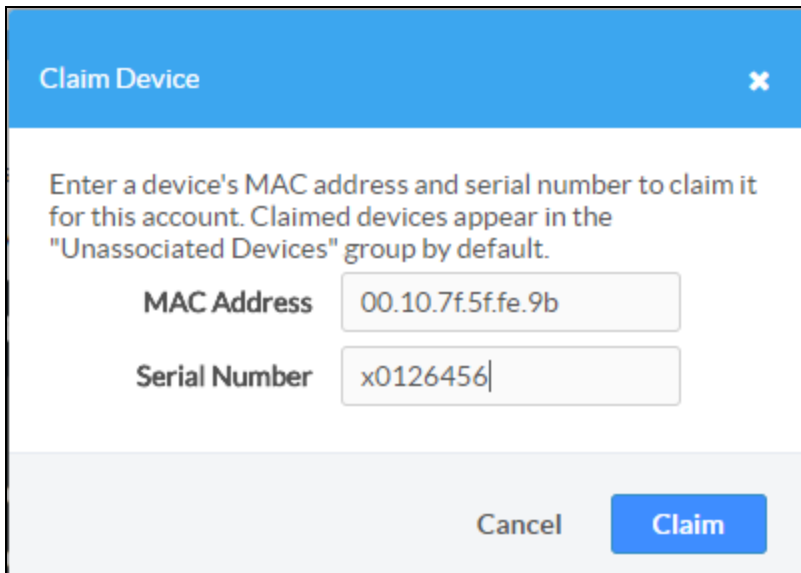
1. Record the MAC address and serial number that are labeled on the shipping box or on a sticker attached to the device. The MAC address and serial number are required to add the device to the XiO Cloud environment.
2. Open a web browser, and log in to the XiO Cloud service at <https://portal.crestron.io>.
3. Click the **ENVIRONMENT** menu button (☰) to display the **Environment** menu.

Environment Menu



4. Click **Claim Device**. The **Claim Device** dialog box is displayed.

Claim Device Dialog Box



Claim Device

Enter a device's MAC address and serial number to claim it for this account. Claimed devices appear in the "Unassociated Devices" group by default.

MAC Address 00.10.7f.5f.fe.9b

Serial Number x0126456

Cancel Claim

5. Enter the MAC address and serial number recorded in step 1 in the MAC Address and Serial Number fields, respectively.
6. Click **Claim**. A message indicating a successful claiming is displayed.

NOTE: If an error message displays stating the device does not exist, connect the device to a network that has access to the Internet, wait 15 minutes, and then try again.

7. Click **X** to close the dialog box. The host name of the claimed device appears in the device tree under the group **Unassociated Devices**.

The device can now be managed or assigned to a group. For information on creating environments, managing devices, and managing users with the XiO Cloud service, refer to the [XiO Cloud Service User Guide](#) (Doc. 8214).

Claim Multiple Devices

1. Record all of the MAC addresses and respective serial numbers in a comma delimited, CSV file, and then save it to a location that is accessible to the computer used to access the XiO Cloud service. The CSV file should be formatted as shown below:

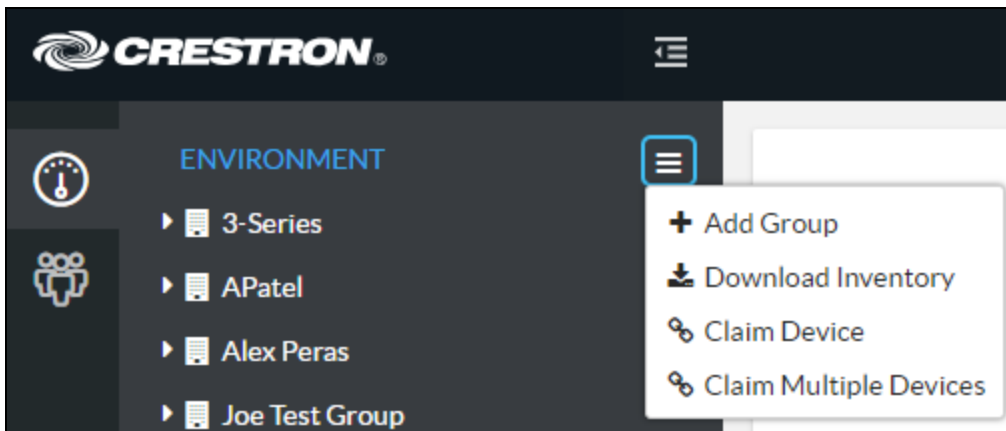
CSV File Format

```
MAC Address,Serial Number
00.10.7e.8b.81.b6,17284712
00.10.7e.8b.8c.87,17284570
00.10.7e.96.83.93,1716JBG01207
00.10.7e.96.92.0a,1716JBG01550
00.10.7e.8b.87.c1,17284670
```

NOTE: MAC addresses and serial numbers are labeled on the shipping box or on a sticker attached to the device.

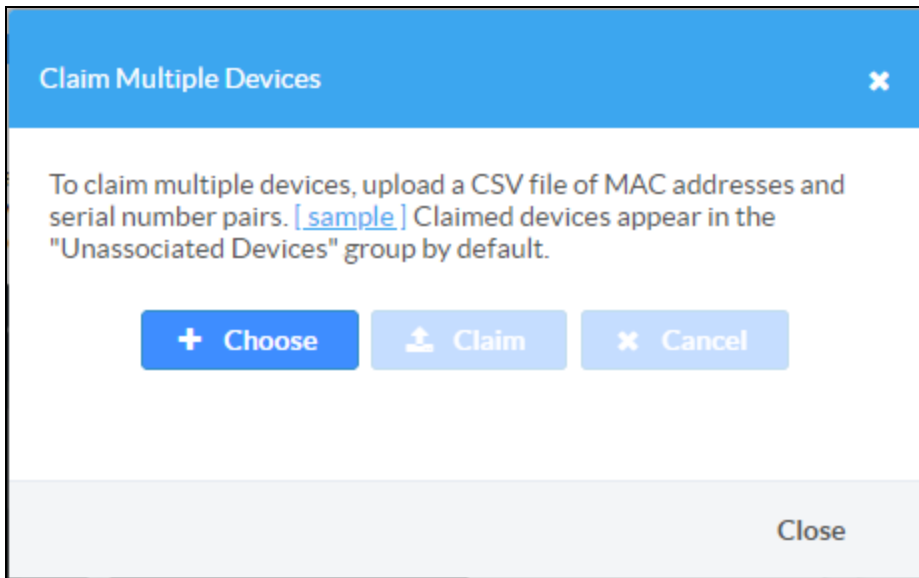
2. Open a web browser, and log in to the XiO Cloud service at <https://portal.crestron.io>.
3. Click the **ENVIRONMENT** menu icon (☰) to display the Environment menu.

Environment Menu



4. Click **Claim Multiple Devices** from the drop-down list. The **Claim Multiple Devices** dialog box is displayed.

Claim Multiple Devices Dialog Box



5. Click **Choose** and select the CSV file created in step 1.
6. Click **Claim** to claim all of the devices listed in the file. A message indicating the claim status of each device is displayed.

NOTE: If an error message displays stating the device does not exist, connect the device to a network that has access to the Internet, wait 15 minutes, and then try again.

7. Click **X** to close the dialog box. The host names of the claimed devices appear in the device tree under the group **Unassociated Devices**.

The devices may now be managed or assigned to a group. For information on creating environments, managing devices, and managing users with the XiO Cloud service, refer to the [XiO Cloud User Guide](#) (Doc. 8214).

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 AM-200 and AM-300 devices, and then use PowerShell® task-based command-line shell and scripting language to configure the devices across a local network.

Operation

On their own, the AM-200 and AM-300 can present content via the following connections:

- A device connected to the HDMI INPUT port
- A device connected to the DM IN port (AM-300 only)
- Crestron AirBoard Whiteboard Capture System
- AirMedia wireless presentation

By default, the AM-200 and AM-300 present the input that was last connected. Optionally, a TSW touch screen (sold separately) can be used to control the system and select which sources are displayed. Additionally, a keypad (sold separately) can be used to adjust volume and turn the system on or off. For instructions on using a touch screen, refer to [Touch Screen Operation \(below\)](#). For instructions on using a keypad, refer to [Keypad Operation \(on page 126\)](#). Otherwise, continue below.

Connect a Source

Connect a source to the HDMI INPUT port, any of the inputs on a connected DM transmitter (AM-300 only), or an AirMedia wireless connection. Its content is shown on the display device.

NOTE: If the AirMedia Canvas feature is enabled and a second source is connected, the second connected source is shown next to the first connected source. For details on configuring AirMedia Canvas, refer to [AirMedia Canvas \(on page 95\)](#).

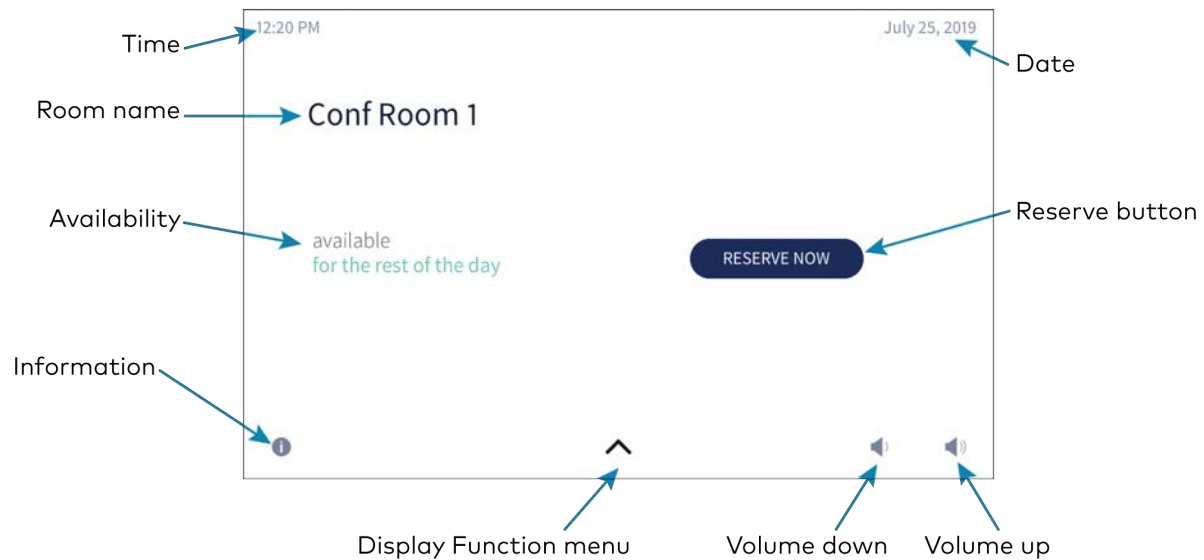
Touch Screen Operation

While the AM-200 and AM-300 always displays the last connected source, a connected touch screen can be used to switch the system power, switch between sources, and adjust volume. The home screen is displayed when the system starts.

NOTES:

- Depending on the configuration, some functions described here may not be available.
- All touch screen displays shown on the following pages reflect the .AV Framework 2.0 theme. To switch the touch screen display to the .AV Framework 1.0 theme, follow the instructions in [General \(on page 71\)](#).

Home Screen




Touch Screen Controls

The following controls are built into the touch screen.

System Power

Tap  to turn on system power. Tap again to turn off system power.

Home Screen

Tap  to return to the home screen.

Screen Controls


The footer contains controls that are always available.

Information

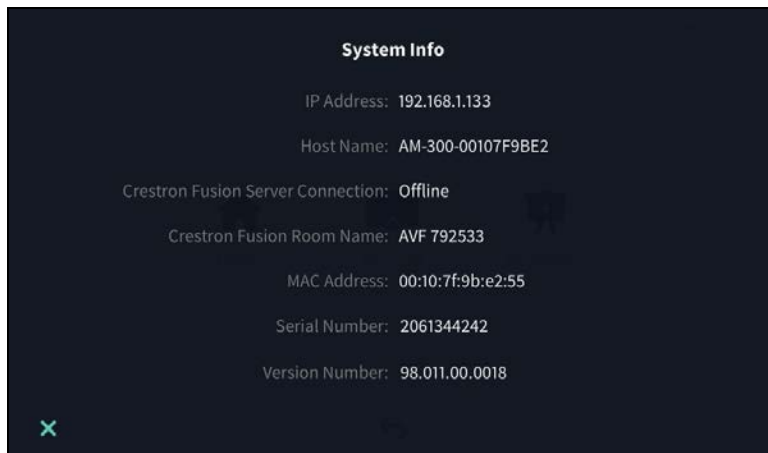
Tap  to view information about the device.

Information screen





Press and hold  to view the System Info screen.

System Info screen




Volume

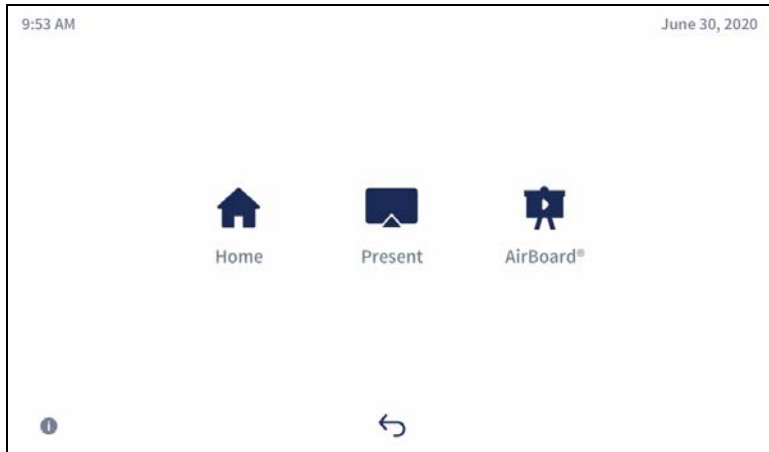
Tap  or  to raise or lower the volume.




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

The Function Menu

Tap  to display the function menu.

Function Menu



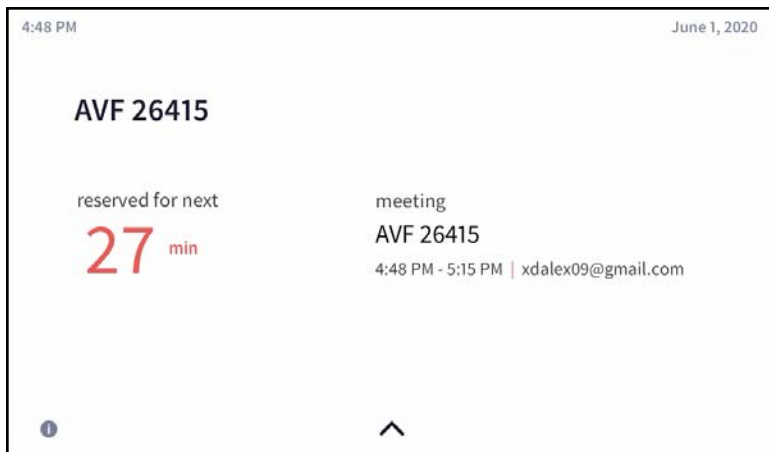
- Tap  (**Home**) to display the Home screen.
- Tap  (**Present**) to view presentation options. For details, refer to [Present Content \(on page 116\)](#).
- Tap  (**AirBoard®**) to share whiteboard content using the Crestron AirBoard Whiteboard Capture System. For details, refer to [Present from the Crestron AirBoard Whiteboard Capture System \(on page 118\)](#).

Schedule a Meeting

The Home screen is used to reserve the conference room.

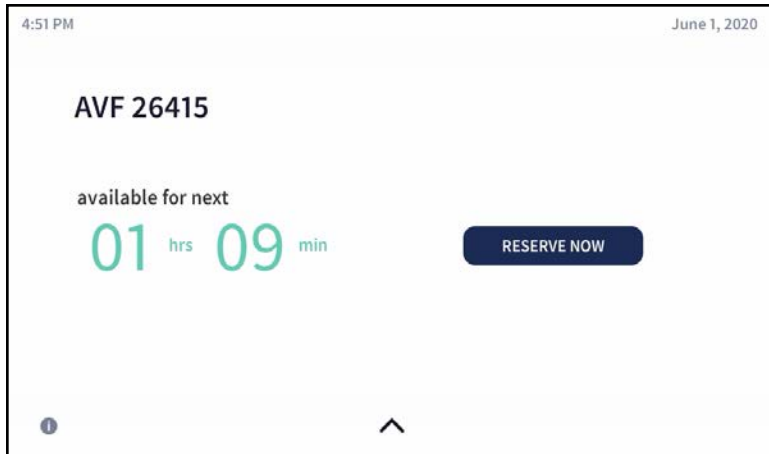
Tap  to display the Home screen. The Home screen displays the current status of the room.

Home Screen – Reserved Room

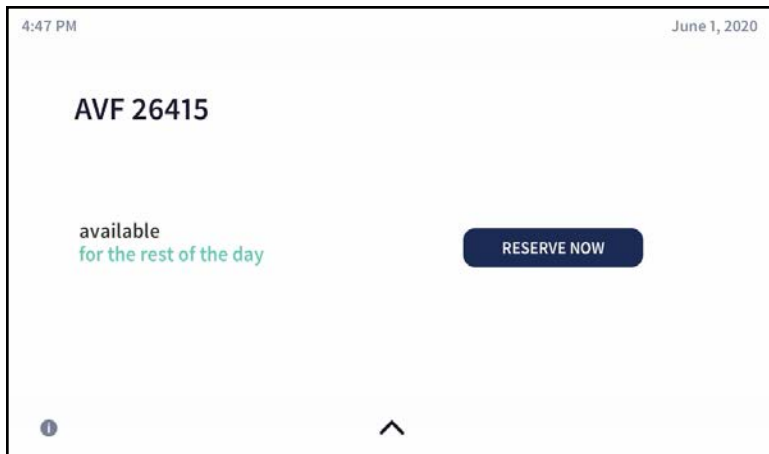


If the room is available for use, the display on the device indicates as such.

Home Screen – Available Room – Limited Time



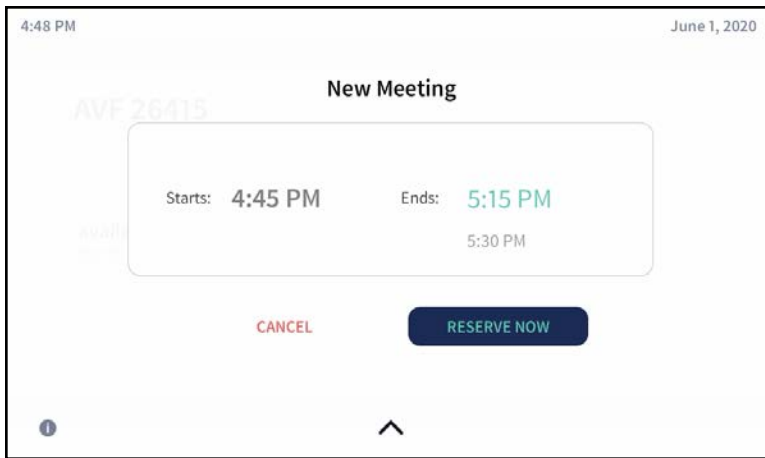
Home Screen – Available Room – Remainder of Day



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

1. Tap **RESERVE NOW** > to reserve the room. The **New Meeting** screen is displayed.

New Meeting Screen



The meeting start and end times are automatically populated for the next available 30-minute block (e.g., 4:45 to 5:15, 5:45 to 6:15, 6:00 to 6:30, etc.). When reserving a meeting space within a current 30-minute block, the start time is rounded down to the nearest 5-minute increment. For example, tapping **RESERVE NOW** at 4:44 pm creates a meeting with a start time of 4:40 pm. If **RESERVE NOW** is tapped at 4:46 pm, the meeting start time would be 4:45 pm. The meeting end time may be set by the user.


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

2. Scroll through the available end times to select the duration of the meeting. The room may 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 book the room.

Present Content

Depending on the configuration, the system can present content from connected HDMI and DigitalMedia sources as well as content streamed from the Crestron AirBoard Whiteboard Capture System or wireless devices over AirMedia. To view the different presentation options, tap . The **Present a Source** screen is displayed.

Present a Source Screen



If any sources are presenting to the display device, they are shown on the touch screen.

Present a Source Screen – Two Sources Showing





Tap a source to have it present on the display device.

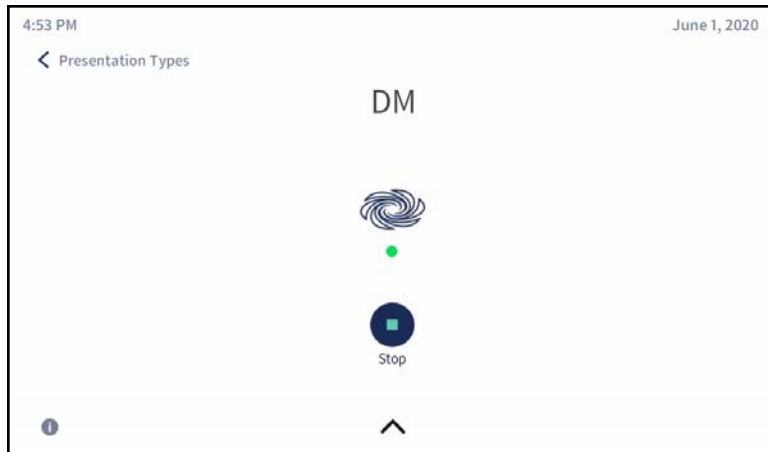
Tap  (**Stop**) to stop a source from presenting on the display device.

NOTE: The Crestron AirBoard source will not be indicated as presenting unless the Crestron AirBoard session has already been initiated. If you tap the **AirBoard** button on the “Present a Source” page and the session has not been initiated, a session will be initiated, and the source will be routed to the display device.



Present Via DM (AM-300 only)

Tap  (DM) to display content from a device connected to a DM transmitter. When done presenting, tap  (Stop). To return to the previous screen, tap < **Presentation Types**.

DM Screen



Present Via HDMI

Tap  (HDMI) to display content from the device connected to the HDMI INPUT port. When done presenting, tap  (Stop). To return to the previous screen, tap < **Presentation Types**.

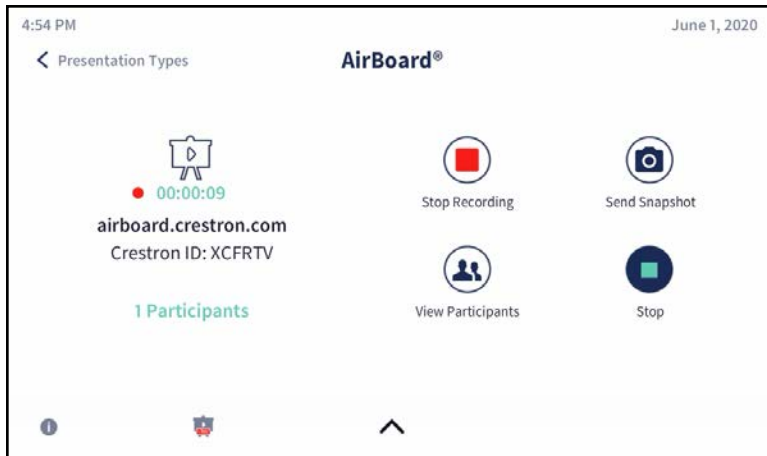
HDMI Screen




Present from the Crestron AirBoard Whiteboard Capture System

Tap  (**AirBoard**) to display content from a paired Crestron AirBoard device. The AirBoard® screen is displayed. When done presenting, tap **Stop Recording**. To return to the previous screen, tap **< Presentation Types**.

AirBoard® Screen



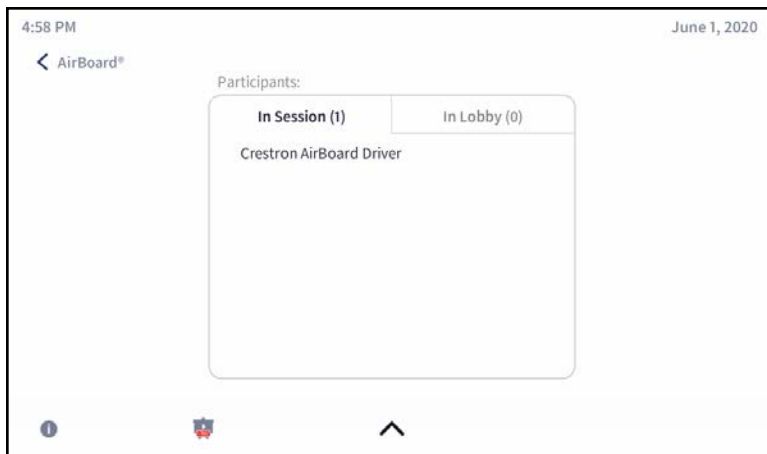
NOTE: The session begins recording immediately upon starting a presentation. Tapping  (**Stop**) stops the presentation, but does not stop the recording session.

While presenting, three features are available from the AirBoard Screen: View Participants, Stop Recording, and Send Snapshot.

View Participants

To see all participants currently viewing the presentation, tap **View Participants**. The Participants screen is displayed. Tap **< AirBoard®** to return to the AirBoard screen.

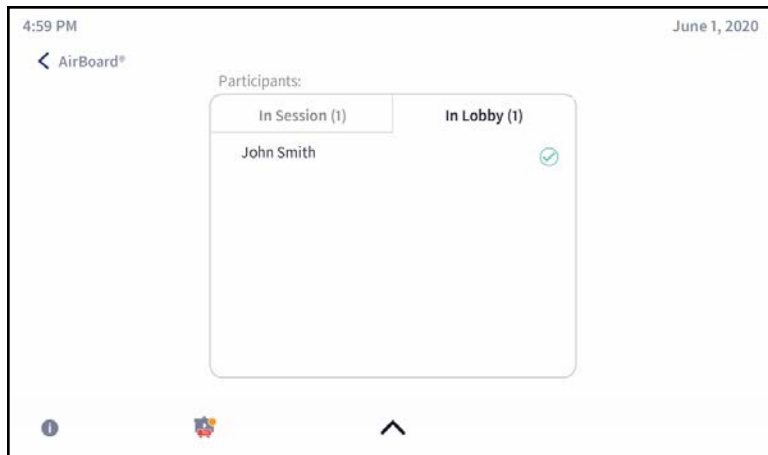
Participants Screen – In Session



Participants can view the presentation on their own web browser software by visiting airboard.crestron.com and entering their name, the Crestron ID of the Crestron AirBoard device, and the code shown on the AirBoard screen. Once a participant has joined the session, their name will be displayed in the In Session section of the Participants screen.

If Code Mode is disabled via the web interface, participants are not required to enter a code in the **Enter Code** field. Instead of directly joining the session, they will be placed into the lobby pending approval on the touch screen before being admitted.

Participants Screen – In Lobby

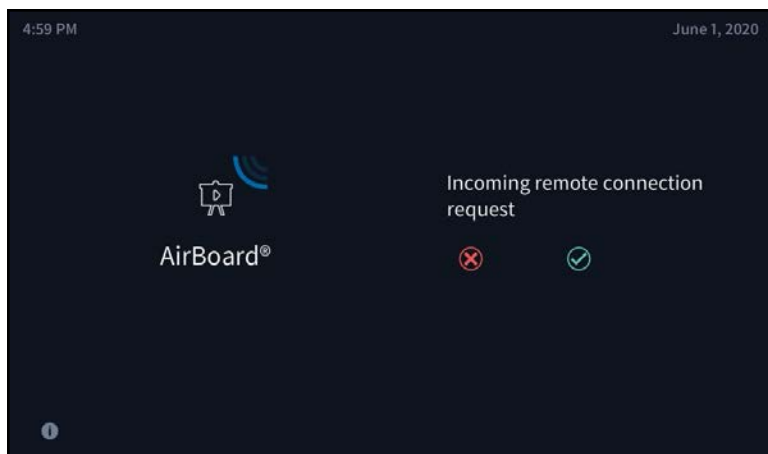




To admit a participant from the lobby into the session, press  beside their name.

NOTE: The maximum number of remote participants is 10.

If a participant requests access while a presentation is not being recorded and the Code Mode is disabled, the following prompt will be shown on the touch screen.

Incoming Remote Connection Request Screen

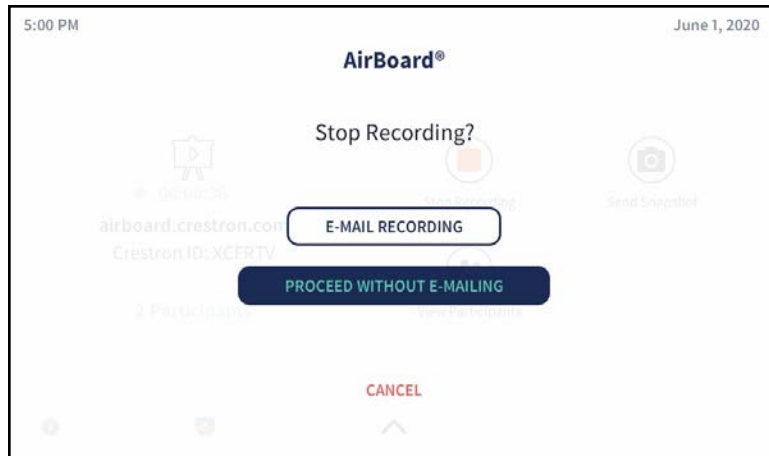


Tap  to deny the request, or tap  to initiate a recording session and admit the participant into the new recording session.

Stop Recording

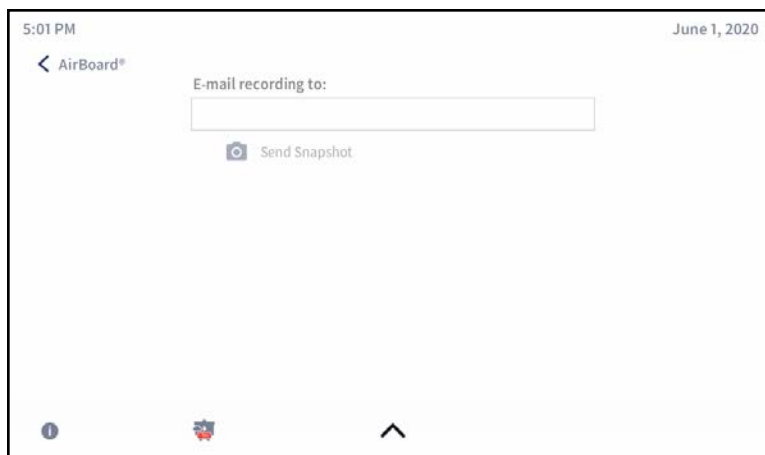
When done presenting, tap **Stop Recording**. The following screen is displayed.

Stop Recording Screen



- To end the session without emailing a recording, tap **PROCEED WITHOUT E-MAILING**.
- To send an email recording of the session, tap **E-MAIL RECORDING**. The E-Mail Recording screen is displayed.

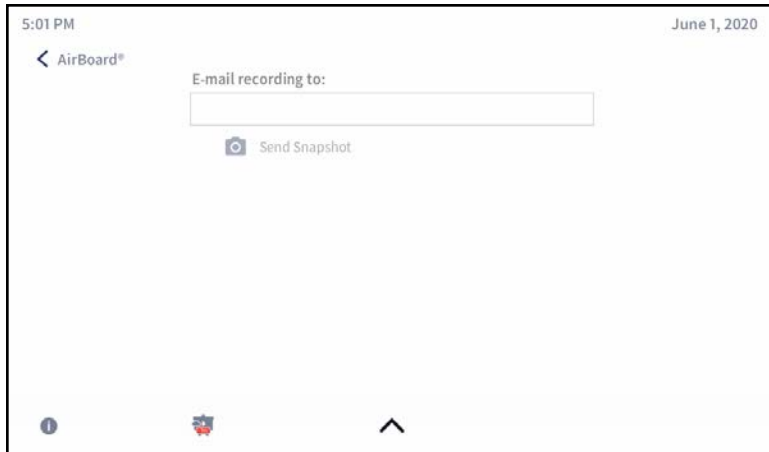
E-Mail Recording Screen



1. Type an email address in the **E-mail recording to:** field. Multiple email addresses may be entered, separated by commas or semicolons.
2. Tap **Send Snapshot** to send an image of the Crestron AirBoard display, or tap **Send Slide Deck** (not shown) to send a slide deck (PDF) of all changes made to the whiteboard.

NOTE: The Send Slide Deck function requires the timeline be enabled and the timeline length be set in the Crestron AirBoard web user interface. Refer to the [CCS-WB-1 Supplemental Guide](#) (Doc. 8323) for details.

E-Mail Recording Screen



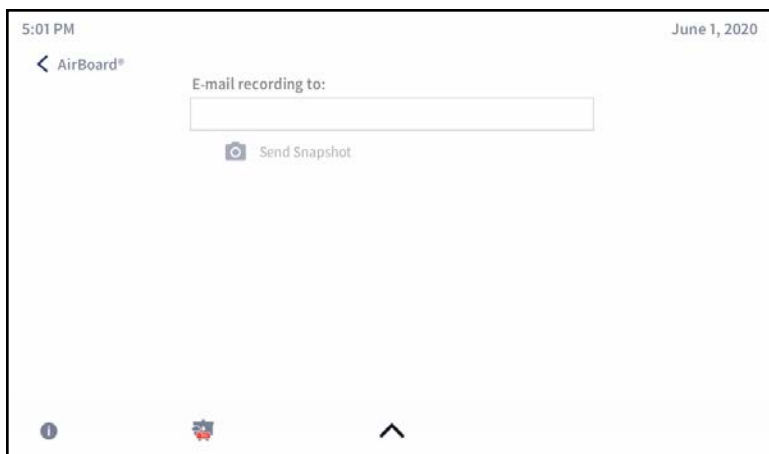
1. Type an email address in the **E-mail recording to:** field. Multiple email addresses may be entered, separated by commas or semicolons.
2. Tap **Send Snapshot** to send an image of the Crestron AirBoard display, or tap **Send Slide Deck** (not shown) to send a slide deck (PDF) of all changes made to the whiteboard.

NOTE: The Send Slide Deck function requires the timeline be enabled and the timeline length be set in the Crestron AirBoard web user interface. Refer to the [CCS-WB-1 Supplemental Guide](#) (Doc. 8323) for details.

Send Snapshot

Tap **Send Snapshot** to send a snapshot of the presentation. The Send Snapshot screen is displayed.

Send Snapshot Screen

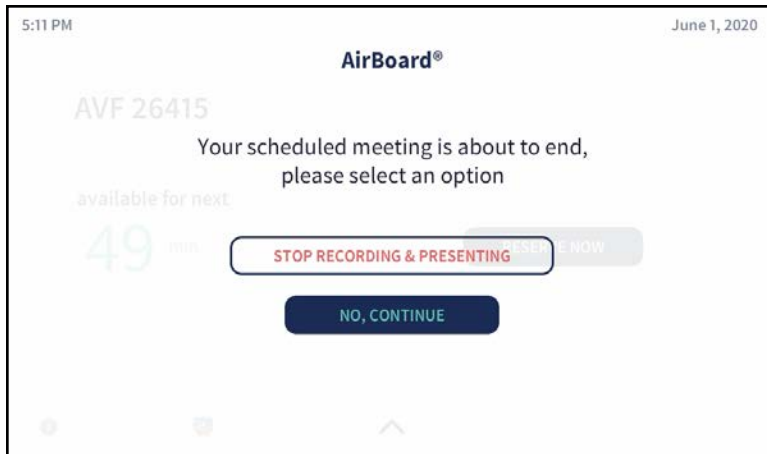


1. Type an email address in the **E-mail recording to:** field.
2. Tap **Send Snapshot** to send an image of the whiteboard in its current state. Multiple email addresses may be entered separated by commas or semicolons.

Meeting Conclusion Warning

When a scheduled meeting is almost over, the following prompt will appear.

Meeting Conclusion Warning

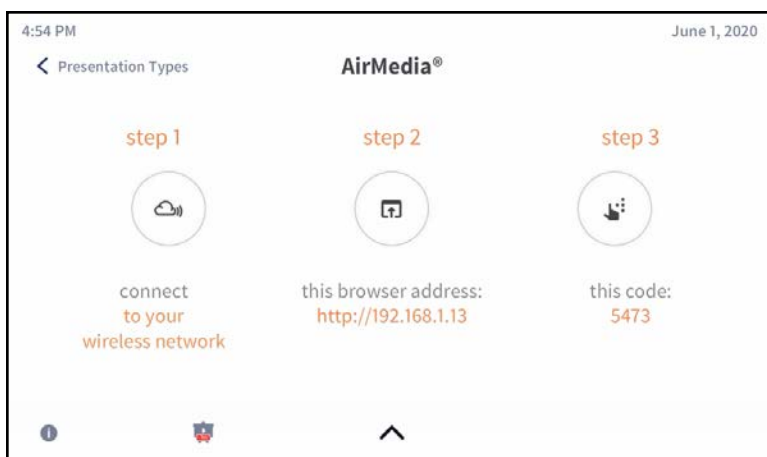


- Tap **STOP RECORDING & PRESENTING** to end the recording and presenting session. Refer to [Stop Recording \(on page 120\)](#) for information on sending recordings to participants once the recording has been stopped.
- Tap **NO, CONTINUE** to continue recording and presenting past the scheduled meeting length.

Present Via AirMedia

Tap **AirMedia** to display content from a device connected through AirMedia. The **Connect to AirMedia®** screen is displayed.

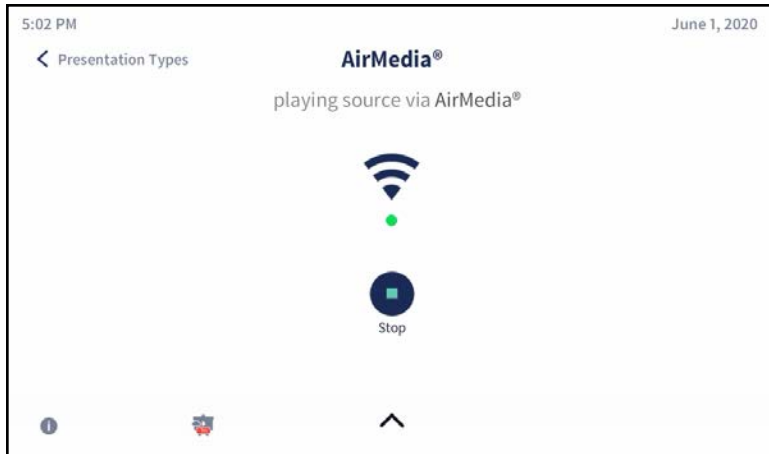
Connect to AirMedia® Screen



Refer to [Use AirMedia \(on page 126\)](#) for instructions on connecting to AirMedia and sharing content.

When sharing content over AirMedia, the following screen is displayed. When done presenting, tap **■ (Stop)**. To return to the previous screen, tap **< Presentation Types**.

Playing Source via AirMedia® Screen



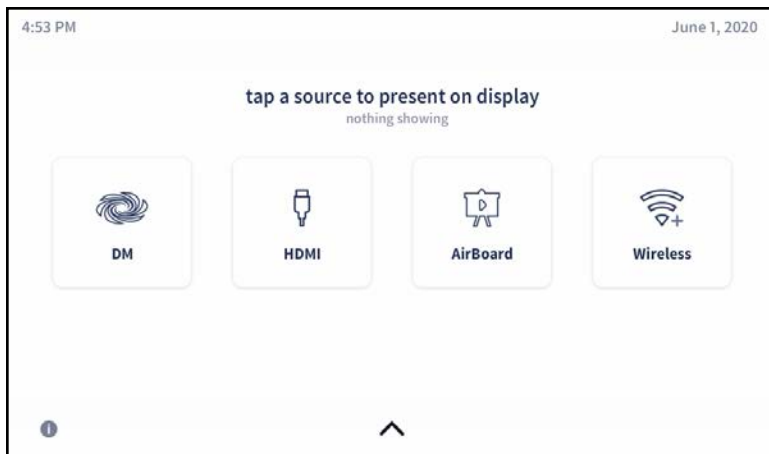
AirMedia Canvas

When configured, the AM-200 and AM-300 can show two 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 AM-200 and AM-300 to use the AirMedia Canvas feature, refer to [AirMedia Canvas \(on page 95\)](#).

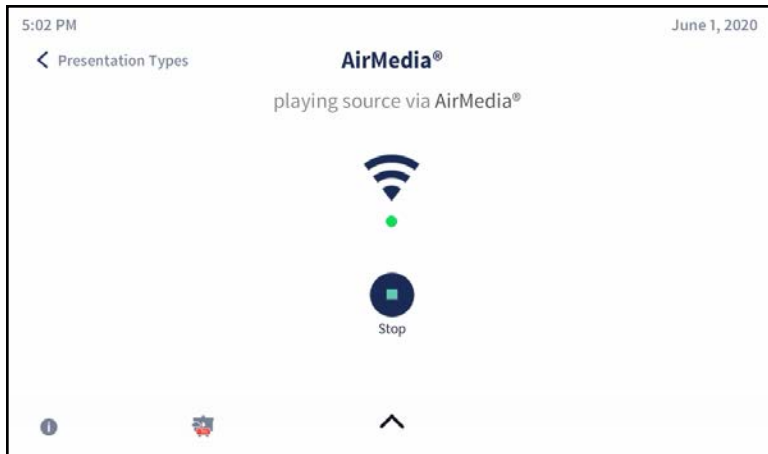
When the AirMedia Canvas feature is enabled, the Present a Source screen appears as shown below.

Present a Source Screen

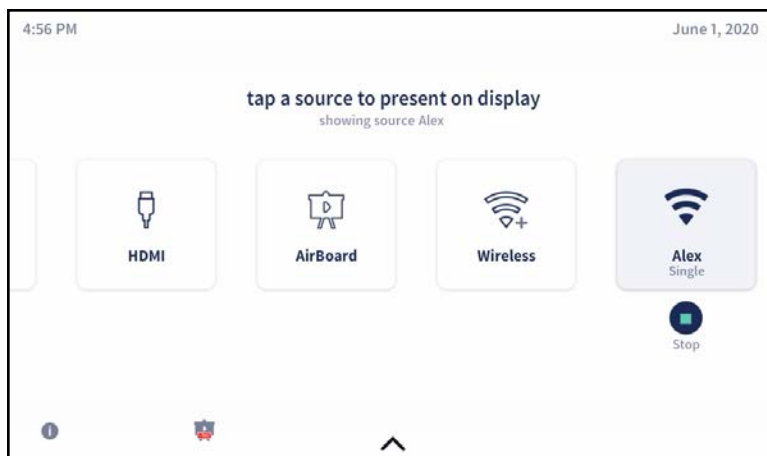


Select Sources

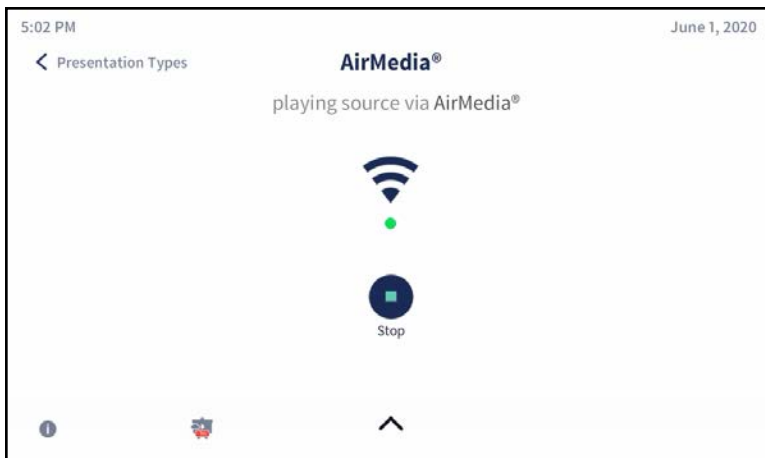
1. Connect all sources to the AM-200 or AM-300.
2. Tap the first source for presentation. The content will appear on the display device.



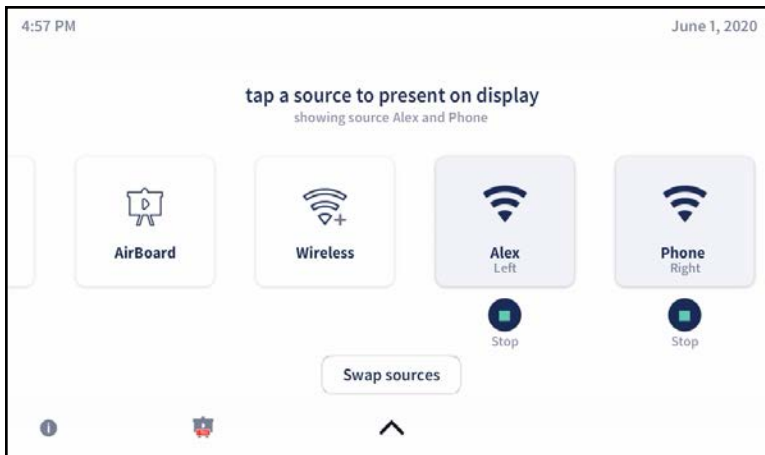
3. Tap < **Presentation Types**. The touch screen will show the connected source.



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




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



6. Tap a third source to disconnect the first source. The display device will show the second and third sources side by side.

Manage Sources

Switch to Single Source

When two sources are shown on the display device, tap  (**Stop**) of the source to be removed 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.

Keypad Operation

While the AM-200 and AM-300 always display the last connected source, a ZUMMESH-KP10AMBATT AirMedia keypad can be used to switch the system power and adjust volume.

NOTE: Zūm devices are available in select markets. For a list of available markets, refer to Answer ID 1000127 in the Online Help section of the Crestron website (www.crestron.com/onlinehelp).

System Power

Tap **ON** to turn on system power. Tap **OFF** to turn off system power.

Volume

Tap **VOLUME UP** to raise the volume. Tap **VOLUME DOWN** to lower the volume.

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

Use AirMedia

The AM-200 and AM-300 use a client application to share a Windows or Mac (hereafter referred to as “computer”) desktop. The computer should 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 or the Crestron PinPoint mobile app, which are 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 in iTunes® software or Google Play™ store.

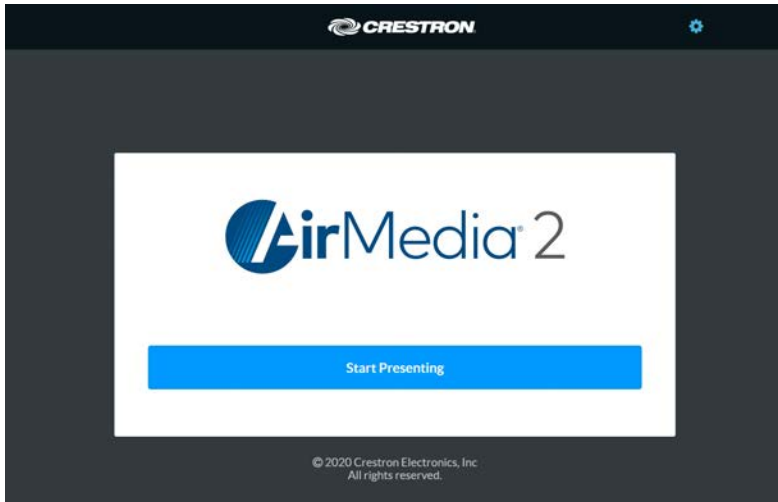
NOTE: For additional details on using AirMedia, refer to the [AirMedia Presentation Gateway Deployment Guide](#) (Doc 7693).

Establish a Connection

From a Computer

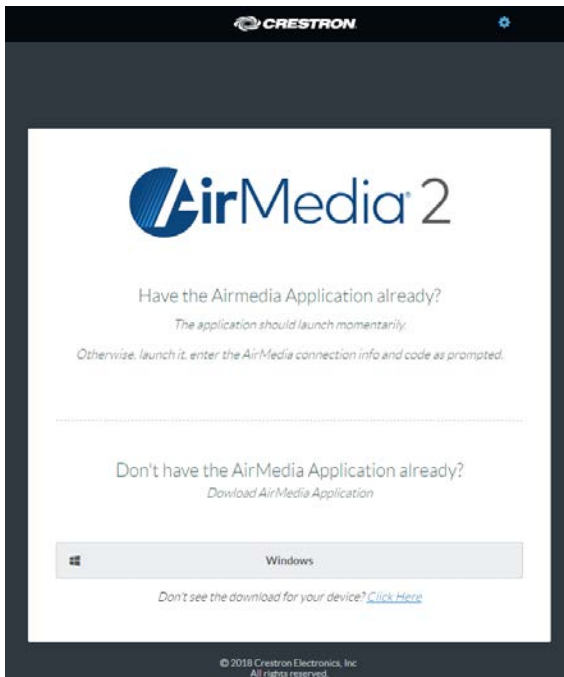
1. Open a web browser on the computer, and navigate to the web address or IP address shown on the display device. The welcome screen is displayed.

Welcome Screen



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

AirMedia 2 Screen



3. Click the icon 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.

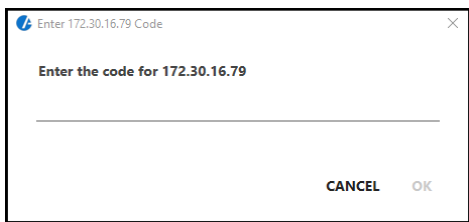
Share Content

From a Windows Computer

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

1. Run the client application. The **Enter Code** dialog box is displayed.

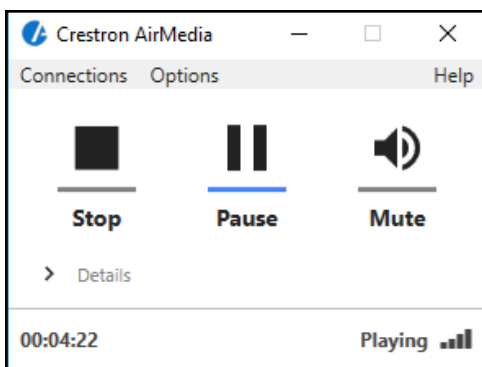
Enter Code Dialog Box





NOTE: If a code is not displayed, the presentation controls are displayed.

2. Enter the code shown on the display device and click **OK**. The client establishes a connection between the computer and the AM-200/AM-300. The client also displays the presentation controls on the computer while the contents of the computer screen are shown on the display device connected to the AM-200/AM-300.

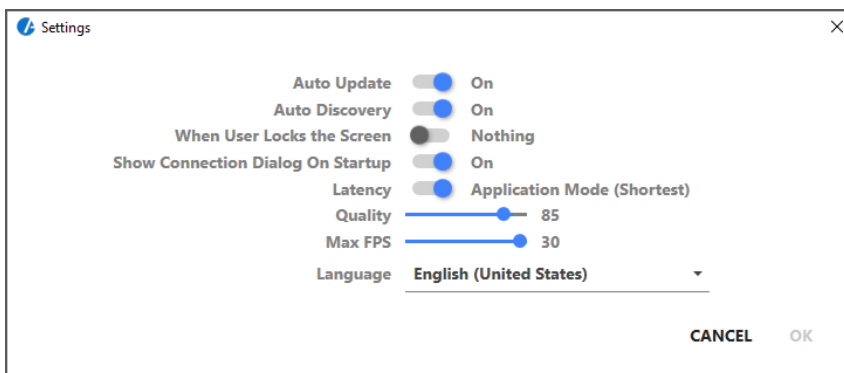
Presentation Controls



3. Direct the presentation with the following controls:
 -  Stop showing the computer's screen.
 -  Start showing the computer's screen.

- **||** Freeze the computer's screen.
- **🔇** Mute the audio output to the device.
- - Minimize the presentation control screen.
- **X** Close the client application and the connection between the computer and the device.
- Click **Details** for additional controls and information.
 - The Video Source control allows the user to select between the primary desktop, additionally attached desktops, or an extended desktop (if available).
 - Information about the connected user, the name of the AM-200 or AM-300 device, the IP address, and the access code are displayed.
- Click **Options > Settings** to customize AirMedia settings. Adjust the settings below and click **OK** to save the changes or click **Cancel** to cancel.

AirMedia Settings Dialog Box



- **Auto Update** should be set to **On**.
- **Auto Discovery** should be set 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).
- **Show Connection Dialog on Startup** selects whether connection information is displayed when the client starts.
- **Latency** selects the amount of latency in transmitting the signal from the computer to the AM-200/AM-300. Select **Application Mode (shortest)** for the least amount of latency (best for slides) or **Video Mode (Pre-Buffer)** for a longer amount of latency, but suitable for buffering shared video.
- 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.

1. Run the client application.
2. Follow the onscreen instructions.

From a Wireless Device

After a connection to the AM-200 or AM-300 has been established using the AirMedia client application on a computer, content can be presented from a wireless device using the Crestron AirMedia app or the Crestron Pinpoint app. Open the app, then follow the onscreen instructions for sharing content.

Using Miracast

Miracast is a mirroring protocol and wireless technology used to project your screen to the AirMedia 2.0 receiver within the AM-200 or AM-300 without the need to install an application on your PC. For instructions on how to use Miracast with the AM-200 or AM-300, refer to the Miracast on AirMedia 2.0 section of the [AirMedia Presentation Gateway Deployment Guide](#) (Doc 7693).

Appendix A: Enabling Modern Authentication for EWS

This appendix provides the procedures required to configure Modern Authentication (OAuth 2) support for the AM-200/AM-300 in the Microsoft® EWS (Exchange Web Services) service.

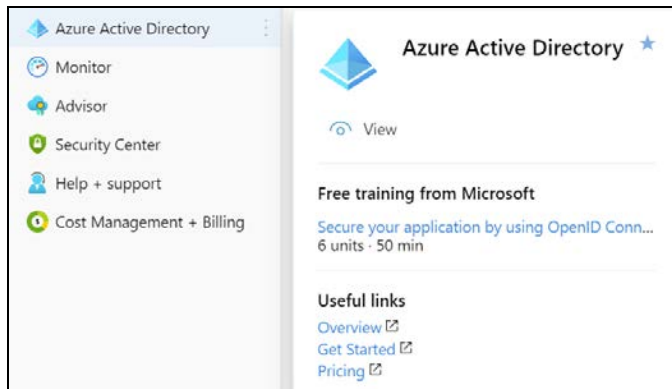
The Modern Authentication authorization model is provided by the Azure® Active Directory® service to integrate managed API applications with the same authentication model used by the Microsoft 365 software REST APIs. Once Modern Authentication is configured in EWS, the AM-200/AM-300 uses this access 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

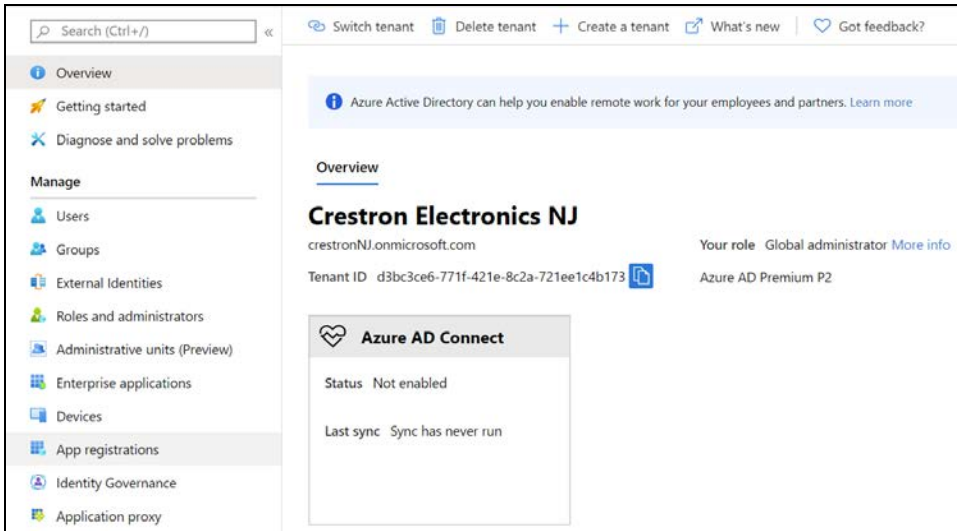
1. Sign into the Azure portal with a user ID with sufficient permissions to create an app.
2. Select **Azure Active Directory** from the left navigation menu.

Azure Active Directory Selection



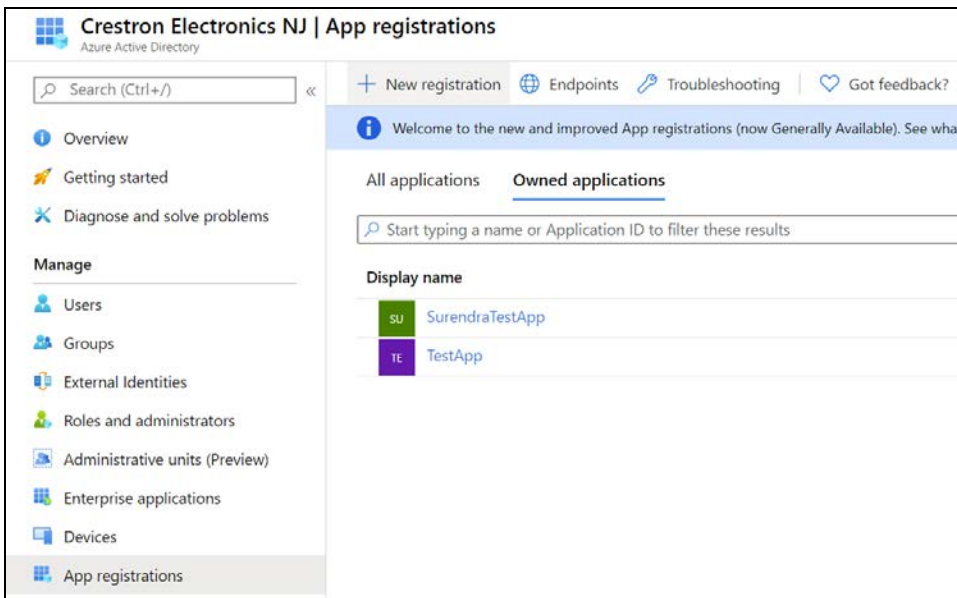
3. Select **App registrations** from the Azure widget menu.

App registrations Selection



4. Click **+ 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 AM-200/AM-300 at this time.

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

6. Click **Register**.

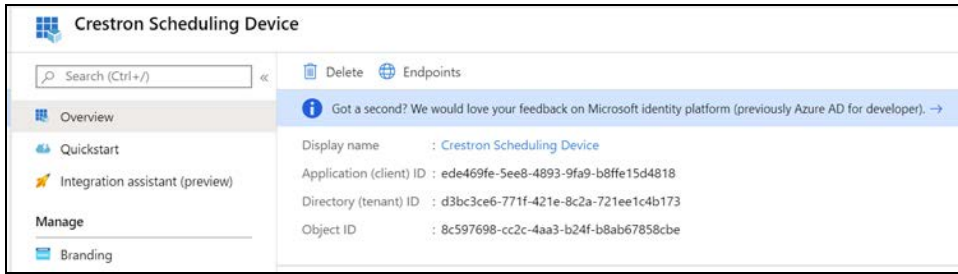
Obtain Authentication IDs

Once the app is registered, the application and directory IDs must be obtained to connect the AM-200/AM-300 to the Azure AD app.

1. Select **App registrations** from the Azure widget menu.
2. Select the application created for the AM-200/AM-300. 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

The screenshot shows the 'Crestron Scheduling Device | Branding' configuration page. The left sidebar contains navigation options: Overview, Quickstart, Integration assistant (preview), Manage (Branding, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, Owners, Roles and administrators (Previ...), Manifest), and Support + Troubleshooting (Troubleshooting, New support request). The main content area includes a search bar, Save/Dismiss buttons, and the following settings:

- Name:** Crestron Scheduling Device
- Logo:** Crestron logo
- Upload new logo:** Select a file
- Home page URL:** https://www.crestron.com
- Terms of service URL:** e.g. https://myapp.com/termservice
- Privacy statement URL:** e.g. https://myapp.com/privacystatement
- Publisher domain:** crestronNJ.onmicrosoft.com (Update 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

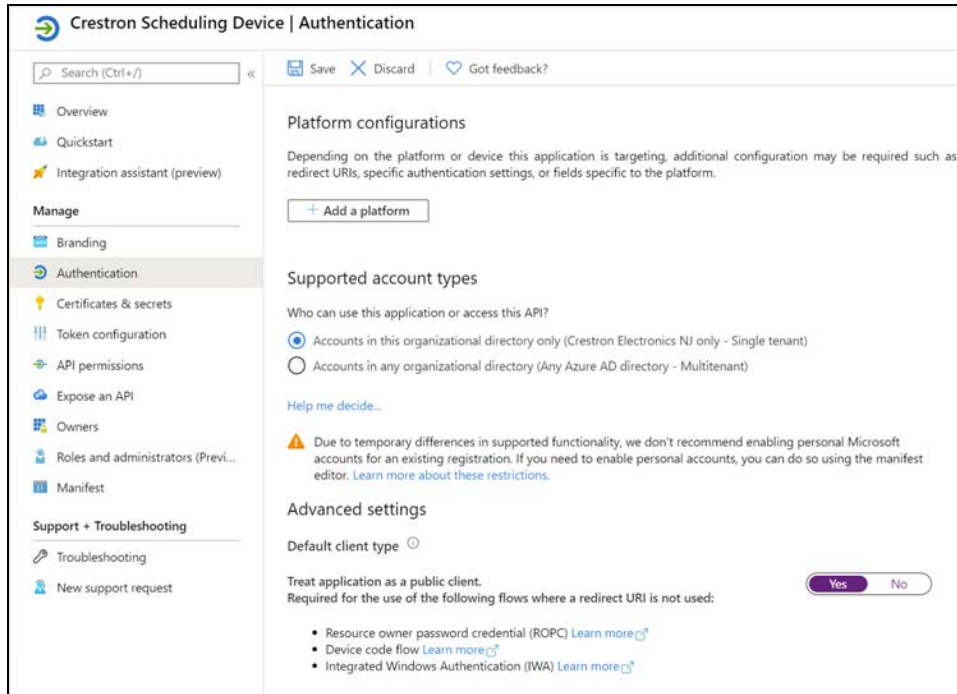
The following branding settings can be configured for the application:

- **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.

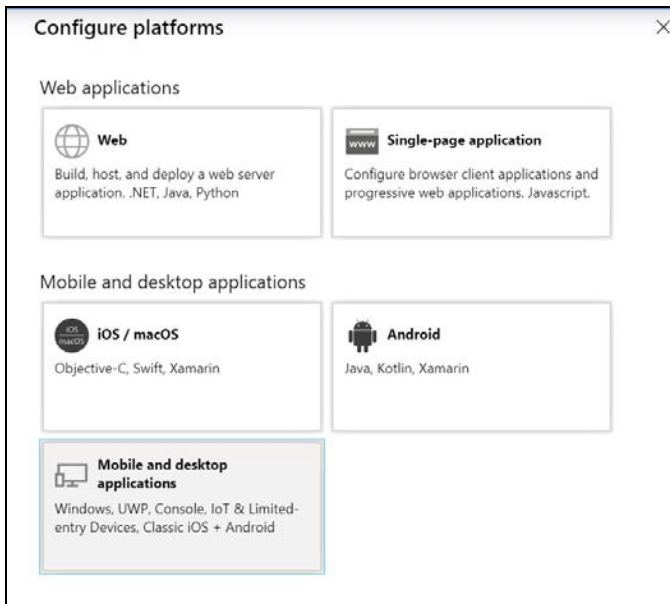
Application Authentication Screen



The following authentication settings can be configured for the application:

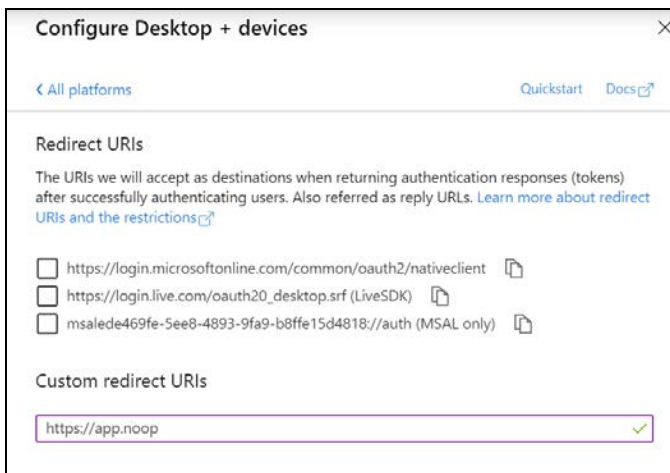
- **Add a Platform:** Click this button to create a platform for app authentication. The **Configure platforms** pane is displayed on the right side of the screen.

Configure platforms Pane



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

Configure Desktop + devices Pane



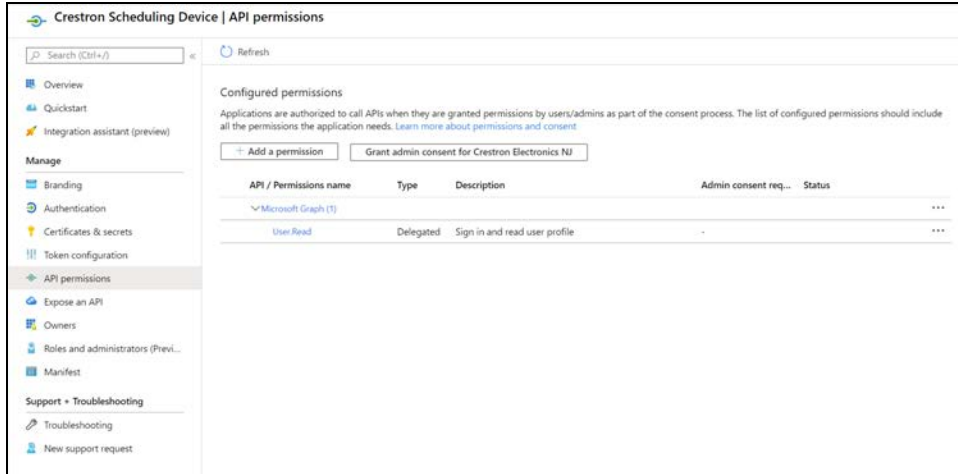
Azure AD requires the use of a redirect URI, but the AM-200/AM-300 does not. Enter a valid URI address and click **Configure**.

- **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.

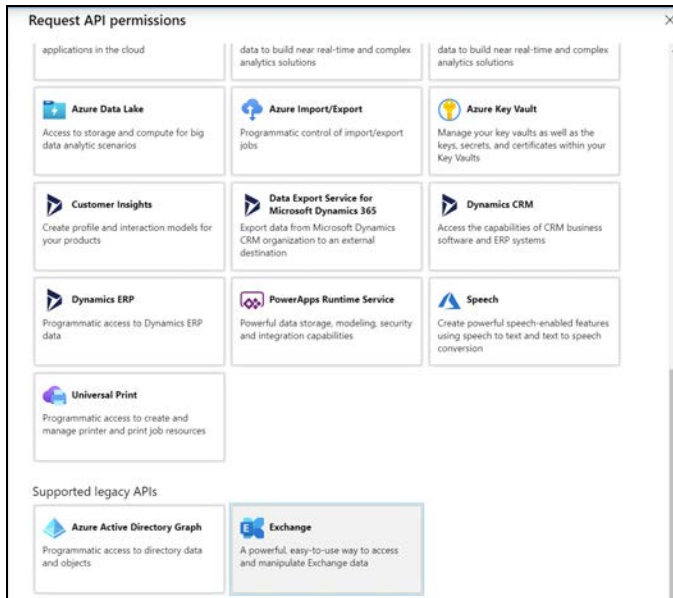
API Permissions Screen



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

Click **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.

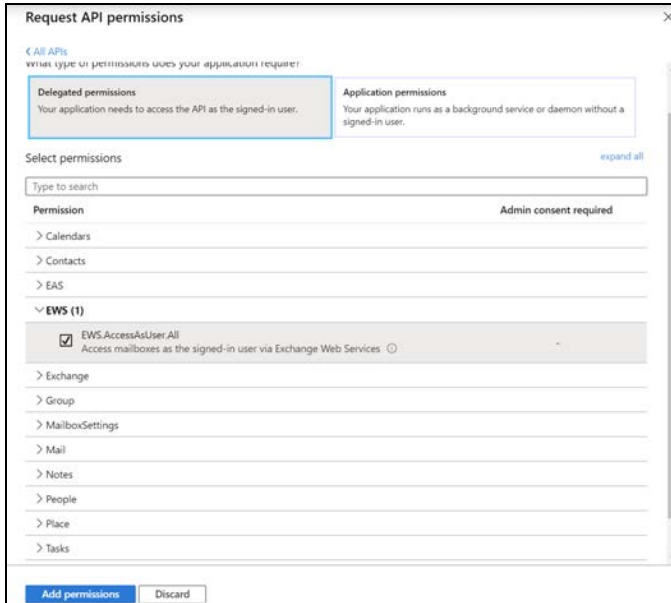
Request API permissions Pane



To set the API permissions for EWS:

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

Request API permissions Pane - Exchange

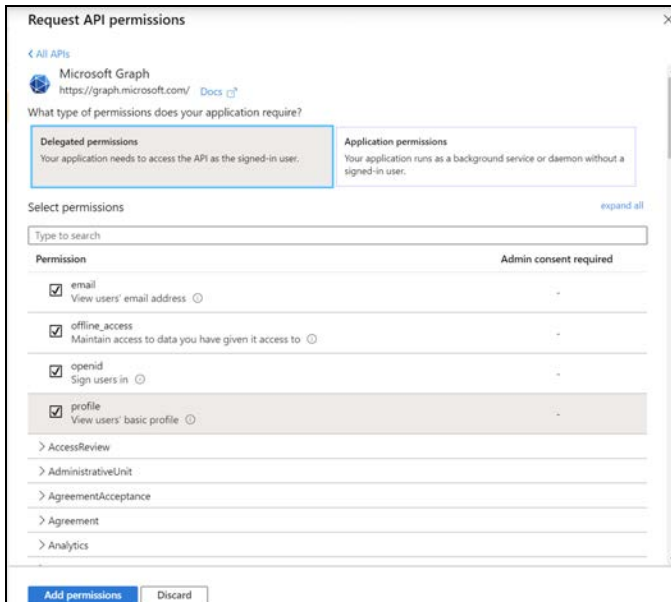


2. Expand the EWS accordion.
3. Fill the checkbox next to **EWS.AccessAsUser.All** to allow the application to make requests to the Exchange Web Services API on behalf of the configured user.

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

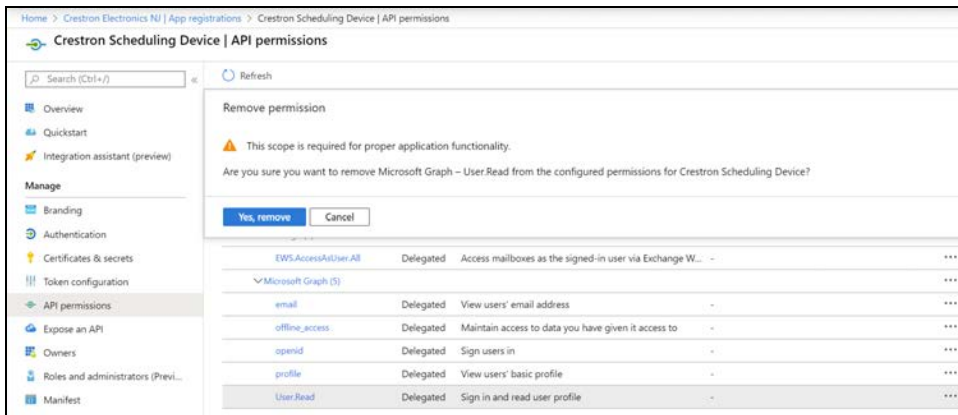


2. Fill the checkboxes next to the following settings to enable the functionality described below:

- **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



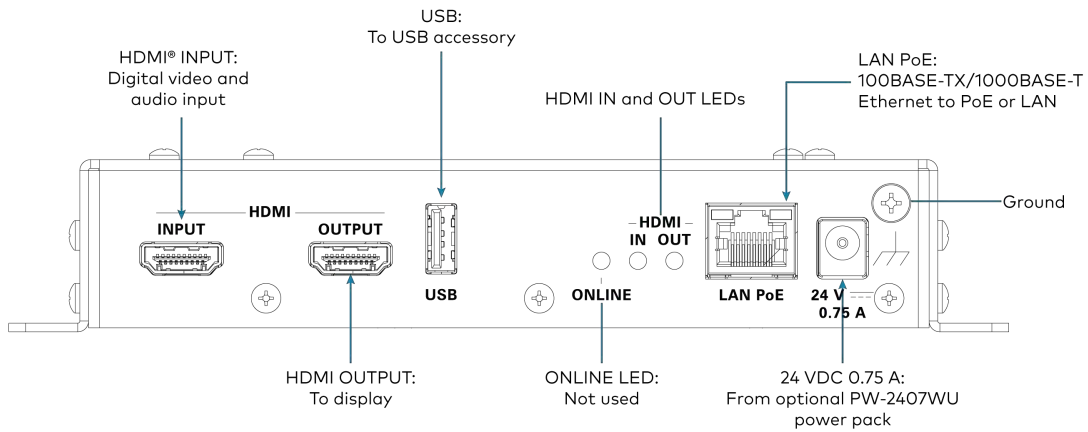
Appendix B: AM-200 and AM-300 Systems

The AM-200 and AM-300 can be used as the centerpiece of an open presentation space. A selection of peripheral devices is available to create a customized presentation space.

Hookup Diagrams

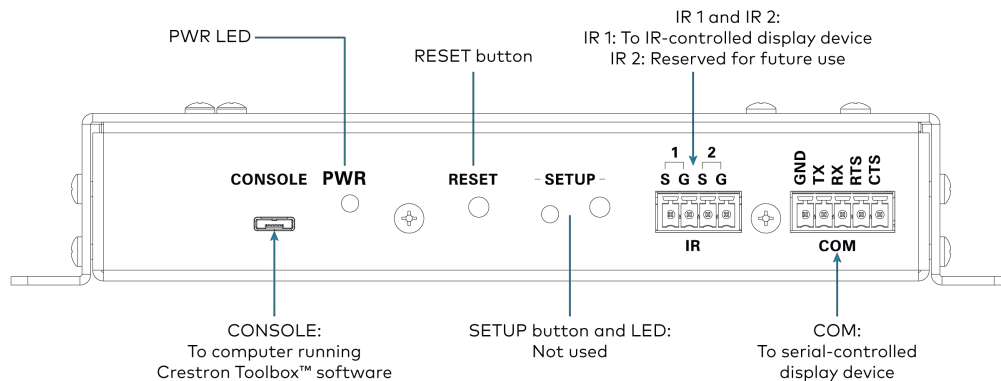
The following diagrams show connections to the AM-200 and AM-300.

AM-200, Top

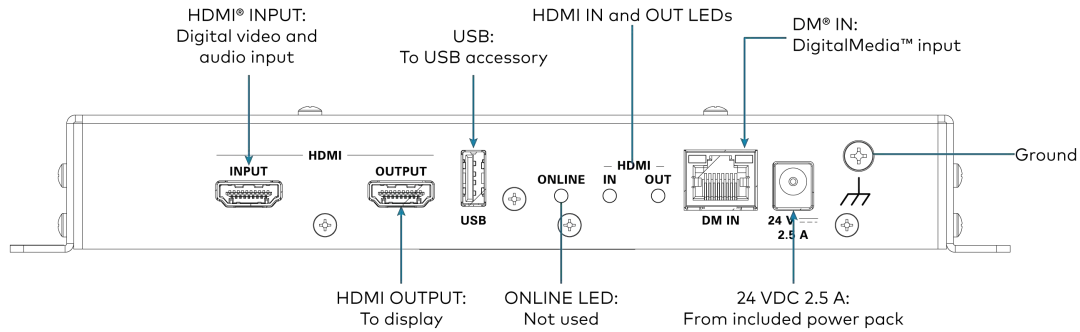


NOTE: The AM-200 can be powered by the optional power pack or by Power over Ethernet (PoE).

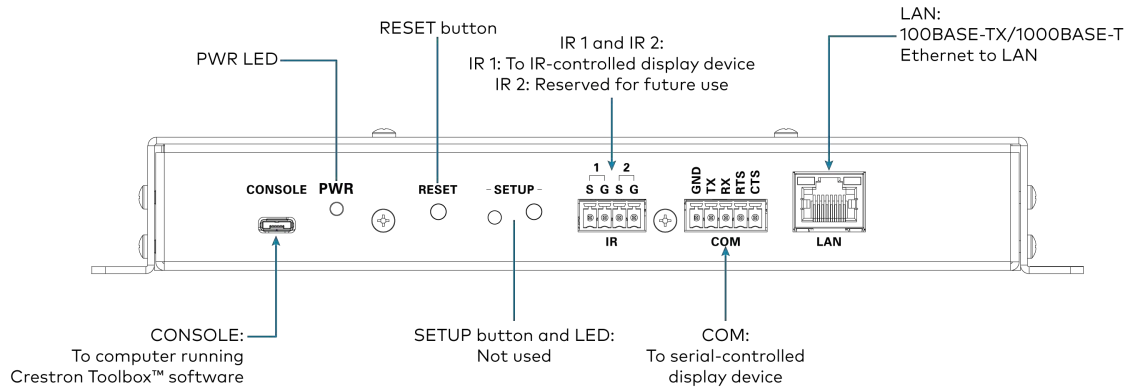
AM-200, Bottom



AM-300, Top



AM-300, Bottom



Supported and Tested DigitalMedia Transmitters (AM-300 Only)

A variety of DigitalMedia transmitters can be used with the AM-300. For a complete list of fully compatible DM transmitters, refer to Answer ID 1000107 in the Online Help section of the Crestron website (www.crestron.com/onlinehelp).

CAUTION: When using a DM transmitter equipped with a LAN port, do not connect the LAN port to the network or a network loop will be created that can disable the network. Only the AM-300 should have a network connection.

Zūm® Devices

NOTE: Zūm® devices are available in select markets. For a list of available markets, refer to Answer ID 1000127 in the Online Help section of the Crestron website (www.crestron.com/onlinehelp).

AM-200 and AM-300 systems can use a Zūm occupancy sensor and keypad for system control. A ZUMMESH-AVBRIDGE Wireless Control Integration Module (sold separately) is required to integrate the occupancy sensor and keypad into a system.

Supported Devices

The AM-200 and AM-300 support the following occupancy sensor and keypad:

- ZUMMESH-PIR-OCCUPANCY-BATT Zūm Wireless Battery-Powered Occupancy Sensor
- ZUMMESH-KP10AMBATT AirMedia Keypad

Add a Zūm Device to the Network

A Zūm device must be added to the system before operation.

NOTE: Zūm devices can be added and managed from the Zūm AMPS page. Refer to [Device Configuration \(on page 88\)](#).

1. Connect the ZUMMESH-AVBRIDGE to the USB port on the AM-200 or AM-300. Refer to [Hookup Diagrams \(on page 141\)](#) for details.
2. Apply power to the AM-200 or AM-300.
3. Insert batteries into the Zūm device(s) that are to be added to the network. Refer to the device's installation guide for instructions.
4. Create a Zūm space with the ZUMMESH-AVBRIDGE.

Press **SETUP** 5 times, then press and hold **SETUP** until the LED on the device lights (about 10 seconds). After approximately 3 seconds, the device LED begins slowly flashing, indicating that it is in Joining mode.

5. Add a device to the network.

- ZUMMESH-PIR-OCCUPANCY-BATT

Press the **TEST** button 3 times, then press and hold the **TEST** button until the LED on the device lights (up to 10 seconds). The ZUMMESH-PIR-OCCUPANCY-BATT is joined to the ZUMMESH-AVBRIDGE.

- ZUMMESH-KP10AMBATT

Press the top button on the keypad 3 times, then press and hold the top button until the LED on the keypad lights (up to 10 seconds). The LED on the keypad will start to flash slowly to indicate that the ZUMMESH-KP10AMBATT is joined to the ZUMMESH-AVBRIDGE.

6. Press a button on any of the devices to exit the Joining mode.

Monitor and Test Zūm Devices

For instructions on monitoring and testing Zūm devices, refer to either [Zūm \(on page 89\)](#) or Answer ID 1000107 in the Online Help section of the Crestron website (www.crestron.com/onlinehelp).

Add a Touch Screen

The AM-200 and AM-300 support the use of a TSW-760 or TSW-1060 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 AM-200 or AM-300 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 AM-200 or AM-300. For instructions on creating an IP table entry, refer to the [TSW-560/TSW-760/TSW-1060 Supplemental Guide](#) (Doc. 7927).

Load a Touch Screen Project File

Load a touch screen project file to the system's touch screen.

For information on downloading the touch screen project file, refer to Answer ID 1000107 in the Online Help section of the Crestron website (www.crestron.com/onlinehelp).

For details on loading a touch screen project file, refer to the [TSW-560/TSW-760/TSW-1060 Supplemental Guide](#) (Doc. 7927).

This page is intentionally left blank.

