

Crestron **CEN-WAP-ABG**  
802.11a/b/g Wireless Access Points  

---

Operations & Installation Guide



This document was prepared and written by the Technical Documentation department at:



Crestron Electronics, Inc.

15 Volvo Drive

Rockleigh, NJ 07647

1-888-CRESTRON

# Contents

<b>802.11a/b/g Wireless Access Points: CEN-WAP-ABG</b>	<b>1</b>
Introduction .....	1
Features and Functions .....	1
Specifications .....	3
Physical Description .....	5
Industry Compliance .....	10
Setup .....	11
Network Wiring .....	11
Supplied Hardware .....	11
Installation .....	11
Hardware Hookup .....	14
Configuration .....	15
Accessing the Configuration Utility .....	15
Using Setup Wizard Configuration Mode .....	18
Using Custom Settings Configuration Mode .....	20
Problem Solving .....	48
Troubleshooting .....	48
Reference Documents .....	50
Further Inquiries .....	51
Future Updates .....	51
Software License Agreement .....	52
Return and Warranty Policies .....	54
Merchandise Returns / Repair Service .....	54
CRESTRON Limited Warranty .....	54



# 802.11a/b/g Wireless Access Points: CEN-WAP-ABG

---

## Introduction

---

**NOTE:** Unless otherwise noted, references in this manual to CEN-WAP-ABG apply to both the CEN-WAP-ABG-1G and CEN-WAP-ABG-CM wireless access points.

---

CEN-WAP-ABG wireless access points enable wireless communication for Crestron® Wi-Fi touchpanels, 2-Series control systems, computers, and other devices. With IEEE 802.11a/b/g support, easy setup, flush-mount installation, and enterprise level security and management capabilities, a CEN-WAP-ABG delivers an ideal wireless access point solution for any application.

## Features and Functions

- Supports 802.11a, 802.11b, and 802.11g protocols
- Single-wire hookup using Power over Ethernet (PoE)
- Secure network with no configuration required
- Web-browser configuration and management
- Enterprise level security
- Built-in DHCP server
- MAC address filtering
- On-board event logging
- SNMP and UPnP configuration and management
- Bridge mode for wireless LAN-to-LAN capability
- Ethernet control system interface
- Front-panel LAN pass-through port (CEN-WAP-ABG-1G only)
- Attractive flush wall mount (CEN-WAP-ABG-1G) or low-profile ceiling mount (CEN-WAP-ABG-CM) design

### ***Single-Wire Hookup***

Power over Ethernet (PoE) capability powers a CEN-WAP-ABG through the LAN wiring, eliminating the need for a separate power supply. A Category 5 (CAT5) cable simply connects the wireless access point to a PoE injector (PWE-4803RU), allowing for installation at a convenient location apart from the access point. Alternatively, using the Crestron five-port PoE switch (CEN-SW-POE-5), up to four access points can be powered from a single location, simplifying design and wiring. A third-party PoE source device can also be used to power the access point.

### ***No Configuration Required***

Using a CEN-WAP-ABG, a secure Wi-Fi touchpanel connection can be made quickly and easily right out of the box. Each wireless access point ships with a unique network name and network key printed on a removable sticker on the front of the unit. Entering this information into the touchpanel is all that is required to complete the connection. Multiple access points can be installed in the same vicinity without causing any connection problems.

### ***Web-Browser Configuration and Management***

For applications that require a customized configuration, a CEN-WAP-ABG features built-in browser-based management tools. From any Web browser, the easy setup wizard lets you simply select the scenario, such as a standalone network or a high-security environment, and applies the necessary configuration settings for you. After configuration using the setup wizard is completed, step-by-step instructions are then provided for connecting Crestron Wi-Fi touchpanels to the network. Beyond the wizard, there are more comprehensive configuration and security settings available for advanced users and system administrators.

### ***Enterprise Level Security***

For a secure wireless network in the home or office, a CEN-WAP-ABG supports up to 152-bit WEP encryption as well as more advanced WPA and WPA2 authentication and encryption methods. RADIUS certificates are also supported for a true enterprise level solution.

### ***DHCP Server***

A CEN-WAP-ABG can assign IP addresses automatically to touchpanels and other client devices using DHCP (Dynamic Host Configuration Protocol).

### ***MAC Address Filtering***

Unauthorized devices can be prevented from joining the wireless network, maximizing bandwidth for control and streaming AV signals to support only the touchpanels, computers, and other devices that you specify. MAC filtering increases security without switching to an authentication method with more overhead.

### ***Event Logging***

To assist in troubleshooting, a CEN-WAP-ABG keeps a history of the last 500 client connections, disconnections, and failure events, and includes helpful details such as the reason for a disconnect or failure.

**Bridge Mode**

This useful feature allows a CEN-WAP-ABG to be used to add wireless connectivity to any device with an Ethernet port, or to extend a LAN via a wireless link whenever a CAT5 wire cannot be run.

**Ethernet Pass-Through (CEN-WAP-ABG-1G only)**

An Ethernet port is available on the front of the CEN-WAP-ABG-1G, providing a convenient LAN connection for computers and touchpanels. This port can be disabled via software if not required.

**Specifications**

Specifications for a CEN-WAP-ABG are listed in the following table.

*CEN-WAP-ABG Specifications*

SPECIFICATION	DETAILS
RF Wireless	
RF Transceiver	IEEE 802.11a/b/g; 5.8 or 2.4 GHz 2-way RF; 64, 128, and 152-bit WEP encryption; WPA and WAP2 with TKIP and AES
Transmit Power	Up to 19 dBm
Range	30 feet (10 meters); range and speed vary based upon environmental conditions
Ethernet	10BaseT/100BaseTX, auto-switching, auto-negotiating, auto-discovery, full/half duplex, TCP/IP, UDP/IP, DHCP client and server, SNMP, IEEE 802.3u and 802.3af compliant
Power Requirements	IEEE 802.3af Power over Ethernet, 3.3 W (70 mA) @ 48 VDC
Environmental	
Temperature	32° to 104° F (0° to 40° C)
Humidity	10% to 90% RH (non-condensing)
Heat Dissipation	11 BTU/Hr
Enclosure	Injection-molded plastic, white textured finish CEN-WAP-ABG-1G: Wall mountable using a 1-gang plaster ring (recommended) or electrical box (2.5 inch deep minimum), rack mountable using a third-party rack mount panel*; requires Decora faceplate (not included) CEN-WAP-ABG-CM: Ceiling mountable using a 1-gang plaster ring (recommended) or electrical box (2 inch deep minimum), removable and paintable cover

*(Continued on following page)*

*CEN-WAP-ABG Specifications (Continued)*

SPECIFICATION	DETAILS
Dimensions	
CEN-WAP-ABG-1G (without antenna)	
Height	4.14 in (10.51 cm)
Width	1.74 in (4.40 cm)
Depth	2.87 in (7.29 cm)
CEN-WAP-ABG-CM	
Diameter	4.73 in (12.00 cm)
Depth	2.53 in (6.43 cm)
Weight	CEN-WAP-ABG-1G: 5 oz (133 g) CEN-WAP-ABG-CM: 6 oz (168 g)

\* Middle Atlantic HBL1-722243 or equivalent rack mount panel recommended. Note unit dimensions when specifying any other rack mount kit.

**NOTE:** Crestron software and any files on the website are for authorized Crestron dealers and Crestron Authorized Independent Programmers (CAIP) only. New users may be required to register to obtain access to certain areas of the site (including the FTP site).

## Physical Description

This section provides information about the connections, controls and indicators available on your CEN-WAP-ABG.

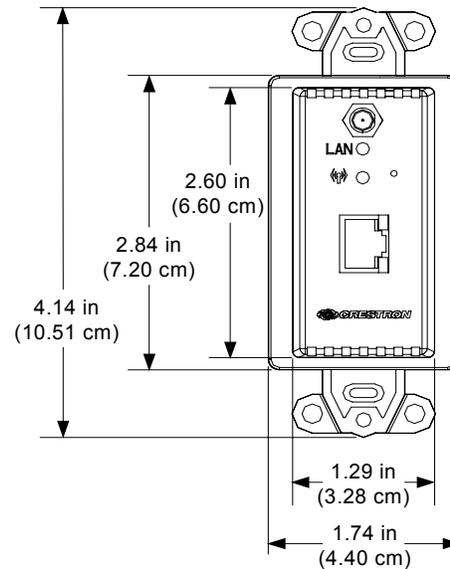
### CEN-WAP-ABG-1G

Information about the connections, controls and indicators of the CEN-WAP-ABG-1G follows.

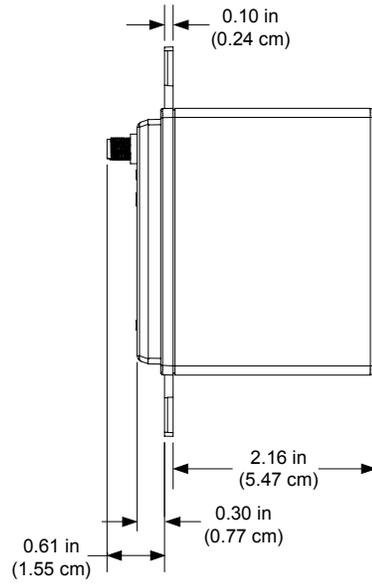
#### CEN-WAP-ABG-1G Physical View (Front and Rear)



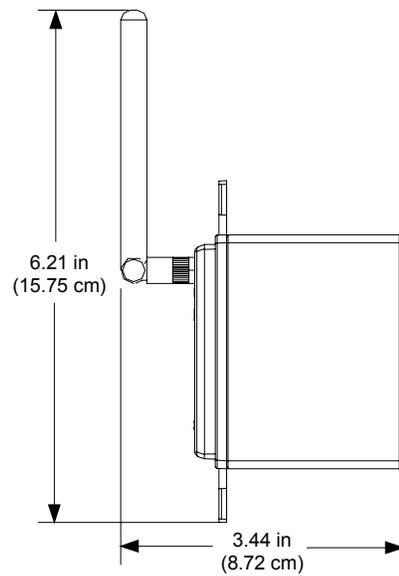
#### CEN-WAP-ABG-1G Overall Dimensions (Front View)



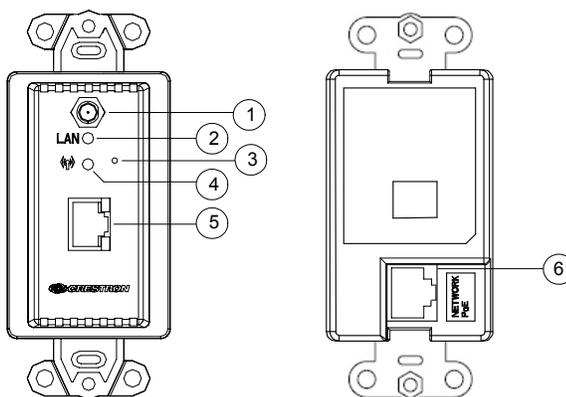
*CEN-WAP-ABG-1G Overall Dimensions (Side View without Antenna, Left)*



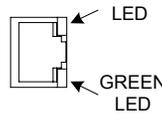
*CEN-WAP-ABG-1G Overall Dimensions (Side View with Antenna, Left)*



*CEN-WAP-ABG-1G Connectors, Controls & Indicators (Front and Rear)*



*Connectors, Controls & Indicators*

#	CONNECTORS, CONTROLS & INDICATORS	DESCRIPTION
1	Antenna	(1) Connects to supplied antenna.
2	LAN	(1) Green LED: Solid green indicates link status of the rear Ethernet port; Flashing green indicates Ethernet activity through the rear Ethernet port.
3	Reset	(1) Recessed push button that resets the device.*
4	Wi-Fi 	(1) Green LED: Solid green indicates wireless network connection; Flashing green indicates wireless data activity.
5	 AMBER LED GREEN LED	(1) 8-wire RJ-45 connector with 2 LED indicators; 10BaseT/100BaseTX Ethernet port; Amber LED indicates 100BaseT link status; Solid green LED indicates link status; Flashing green LED indicates Ethernet activity. Connects to local wired Ethernet equipment (optional).
6	NETWORK PoE 	(1) 8-wire RJ-45 connector; 10BaseT/100BaseTX Ethernet and PoE input port; Connects to IEEE 802.3af-compliant PoE power source.

\* To press the **Reset** button, use the end of a paper clip. Pressing the **Reset** button for eight seconds resets the configuration settings of the unit to factory-default settings.

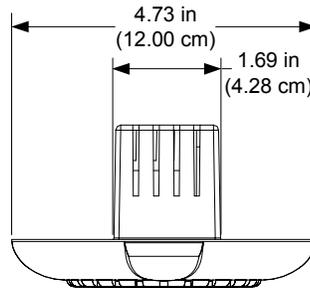
**CEN-WAP-ABG-CM**

Information about the connections, controls and indicators of the CEN-WAP-ABG-CM follows.

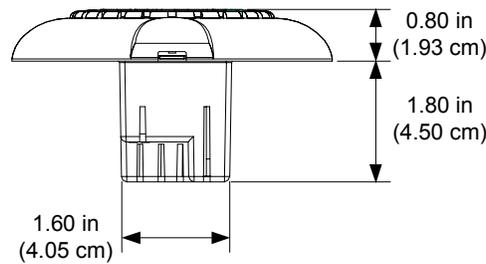
**CEN-WAP-ABG-CM Physical View (Front and Rear)**



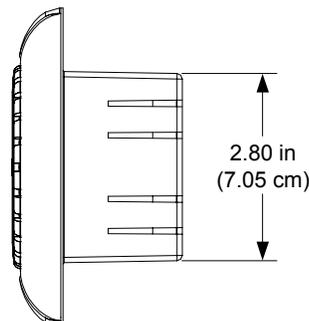
**CEN-WAP-ABG-CM Overall Dimensions (Top View)**



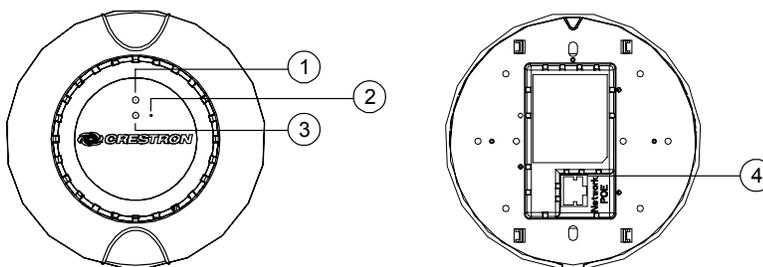
**CEN-WAP-ABG-CM Overall Dimensions (Bottom View)**



**CEN-WAP-ABG-CM Overall Dimensions (Side View, Right)**



*CEN-WAP-ABG-CM Connectors, Control & Indicators (Front and Rear)*



*Connectors, Control & Indicators*

#	CONNECTORS, CONTROL & INDICATORS	DESCRIPTION
1	LAN	(1) Green LED: Solid green indicates link status of the Ethernet port; Flashing green indicates Ethernet activity through the Ethernet port.
2	Reset	(1) Recessed push button that resets the device.*
3	Wi-Fi	(1) Green LED: Solid green indicates wireless network connection; Flashing green indicates wireless data activity.
4	NETWORK PoE 	(1) 8-wire RJ-45 connector; 10BaseT/100BaseTX Ethernet and PoE input port; Connects to IEEE 802.3af-compliant PoE power source.

\* To press the **Reset** button, use the end of a paper clip. Pressing the **Reset** button for eight seconds resets the configuration settings of the unit to factory-default settings.

## Industry Compliance

This product is Listed to applicable UL Standards and requirements by Underwriters Laboratories Inc.



As of the date of manufacture, the CEN-WAP-ABG-1G and CEN-WAP-ABG-CM have been tested and found to comply with specifications for CE marking.



---

**FCC ID: MXF-M930907**

### Compliance Statement (Part 15.19)

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference and
2. This device must accept any interference received, including interference that may cause undesired operation.

### Warning (Part 15.21)

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

### FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

### RF Exposure (OET Bulletin 65)

To comply with FCC's RF exposure limits for general population / uncontrolled exposure, the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

## Setup

### Network Wiring

When wiring the Ethernet network, use CAT5 wiring. CAT5 wiring is a twisted pair cable designed for Ethernet networks. These networks operate at speeds of up to 100 Megabits per second (Mbps) using the 100BaseT standard.

For information on connecting Ethernet devices in a Crestron system, refer to the latest version of the Crestron e-Control<sup>®</sup> Reference Guide (Doc. 6052), which is available for download from the Crestron website ([www.crestron.com/manuals](http://www.crestron.com/manuals)).

### Supplied Hardware

The hardware supplied with a CEN-WAP-ABG is listed in the following table.

#### *Supplied Hardware for a CEN-WAP-ABG*

DESCRIPTION	PART NUMBER	QUANTITY
2.4/5.8 GHz White Omnidirectional Antenna (CEN-WAP-ABG-1G only)	2021159	1
#6-32 x 3/4", Pan Head Phillips Screws	2022188	2

### Installation

#### *Ventilation*

A CEN-WAP-ABG should be used in a well-ventilated area. The venting holes should not be obstructed under any circumstances. Contact with thermal insulating materials should be avoided on all sides of the device. If installing the access point in an insulated wall/ceiling, one inch of insulation must be removed from all sides of the device.

To prevent overheating, do not operate this product in an area that exceeds the environmental temperature range listed in the table of specifications.

#### *Mounting*

This section provides information about mounting the CEN-WAP-ABG-1G and CEN-WAP-ABG-CM as applicable.

#### ***Mounting the CEN-WAP-ABG-1G***

The CEN-WAP-ABG-1G mounts to a wall or into a rack.

#### ***Wall Mounting***

The CEN-WAP-ABG-1G mounts into a one-gang low-voltage bracket or electrical box. The recommended depth of the electrical box is a minimum of 2.5 inches. The maximum voltage of the access point is 48 VDC.

---

**NOTE:** To increase airflow, it is recommended that a low-voltage bracket be used instead of an electrical box.

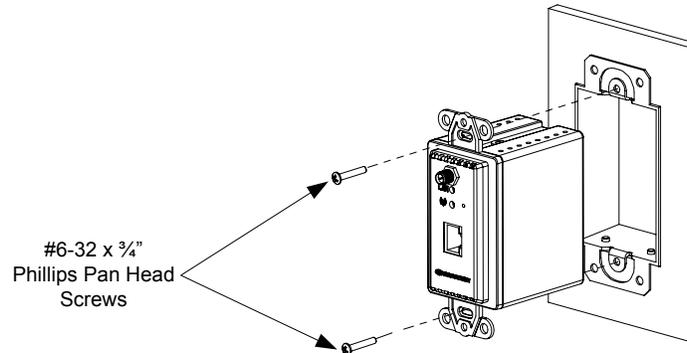
**NOTE:** For the best possible range, it is recommended that you mount the device as high as possible and as far away as possible from metal.

---

To mount the access point into a low-voltage bracket or electrical box (refer to the illustration below):

1. Orient the access point properly, and then place the device into the bracket or electrical box.
2. Attach the access point to the bracket or electrical box using the two #6-32 x 3/4" Phillips pan head screws included with the access point.
3. Attach the desired Decora® faceplate (not included).

***CEN-WAP-ABG-1G Wall Mounting (Low-Voltage Bracket Shown)***



**Rack Mounting**

The CEN-WAP-ABG-1G mounts horizontally into a rack and occupies 1U (1.75 inches) of rack space.

---

**NOTE:** It is recommended that the access point be mounted into a rack only if the connected Wi-Fi devices are to be used less than 20 feet away from the access point and have line of sight to the access point.

**NOTE:** For the best possible range, it is recommended that you mount the device into the topmost rack space.

---

To mount the unit, use the Middle Atlantic HBL1-722243 or equivalent rack mount panel. For ordering information, contact Middle Atlantic Products, Inc. (<http://www.middleatlantic.com>).

***Mounting the CEN-WAP-ABG-CM***

The CEN-WAP-ABG-CM mounts into a one-gang low-voltage bracket or electrical box in the ceiling. The recommended depth of the electrical box is a minimum of two inches. The maximum voltage of the access point is 48 VDC.

---

**NOTE:** To increase airflow, it is recommended that a low-voltage bracket be used instead of an electrical box.

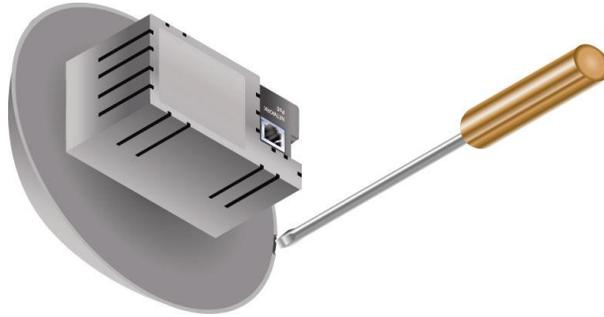
**NOTE:** For the best possible range, it is recommended that you mount the device as far away as possible from metal.

---

To mount the CEN-WAP-ABG-CM to a ceiling:

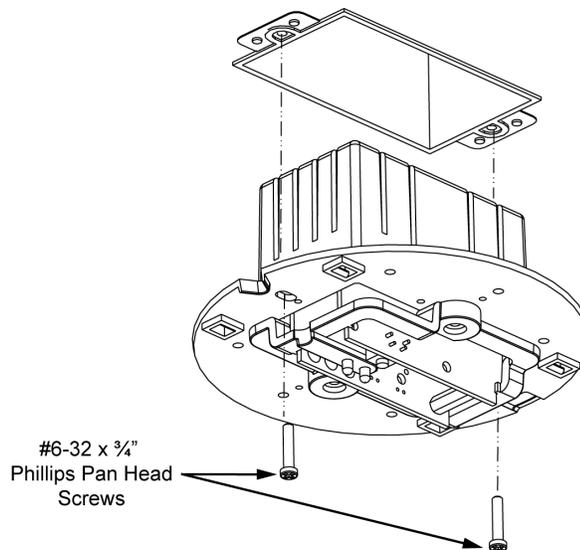
1. Remove the cover by inserting a screwdriver into the notch at the bottom of the access point and pushing the base of the unit upward until it detaches from the cover.

***CEN-WAP-ABG-CM Cover Removal***



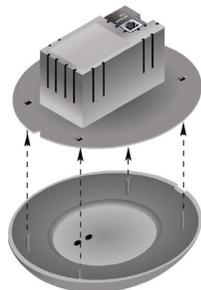
2. Attach the access point to the bracket or electrical box using the two #6-32 x 3/4" Phillips pan head screws included with the access point.

***CEN-WAP-ABG-CM Ceiling Mounting***



3. Reattach the cover by aligning the four tabs inside the cover with the rectangular holes in the base of the access point and pushing the cover until it snaps into place.

***CEN-WAP-ABG-CM Cover Reattachment***



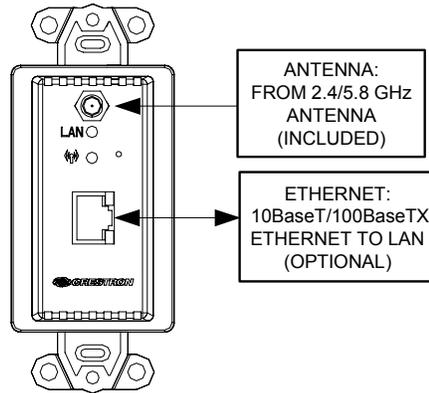
## Hardware Hookup

Make the necessary connections as called out in the following sections. Apply power after all connections have been made.

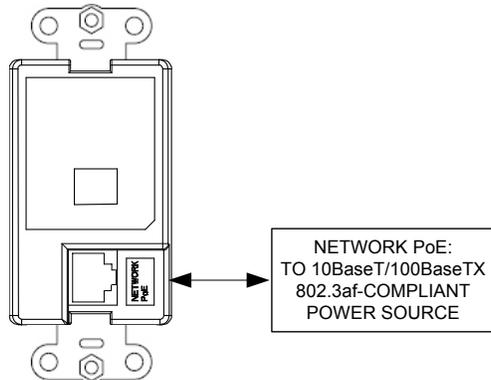
### **CEN-WAP-ABG-1G**

Hardware connections for the CEN-WAP-ABG-1G are shown below.

#### *Hardware Connections for the CEN-WAP-ABG-1G (Front View)*



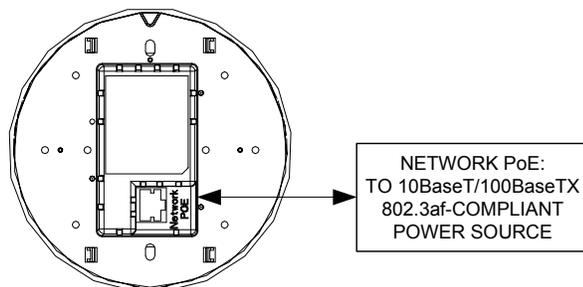
#### *Hardware Connections for the CEN-WAP-ABG-1G (Rear View)*



### **CEN-WAP-ABG-CM**

The hardware connection for the CEN-WAP-ABG-CM is shown below.

#### *Hardware Connection for the CEN-WAP-ABG-CM (Rear View)*



---

## Configuration

---

### Have a question or comment about Crestron software?

Answers to frequently asked questions (FAQs) can be viewed in the Online Help section of the Crestron website. To post a question or view questions you have submitted to Crestron's True Blue Support, log in at <http://support.crestron.com>. First-time users will need to establish a user account.

**NOTE:** A CEN-WAP-ABG is designed to be functional right out of the box. Configure the CEN-WAP-ABG only if customized settings are desired. If customized settings are not desired, refer to the latest version of the CEN-WAP-ABG-1G Quickstart Guide (Doc. 6693) or the CEN-WAP-ABG-CM Quickstart Guide (Doc. 6787), which is available from the Crestron website, for guidelines to connect the access point to Crestron Wi-Fi touchpanels.

---

A CEN-WAP-ABG provides a Web-based utility that can be accessed from a Web browser or from the Crestron Toolbox™. The utility offers two configuration modes:

- Setup Wizard configuration mode, which provides instructions and automated access to the screens necessary to set up a particular configuration or application scenario.
- Custom Settings configuration mode, which allows more advanced configuration than that provided by the wizard and also allows monitoring of the status of the access point.

### Accessing the Configuration Utility

---

**NOTE:** Configuration of a CEN-WAP-ABG must be performed from a computer whose IP address is in the same IP subnet. The default configuration of the access point allows the IP address of the access point to be automatically assigned by a DHCP (Dynamic Host Configuration Protocol) server on the local area network. If a DHCP server does not exist on the network and 45 seconds have elapsed since the access point was powered on, the IP address of the access point defaults to **192.168.1.222** and the subnet mask defaults to **255.255.255.0**.

---

You can access the configuration utility from a Web browser or from the Crestron Toolbox:

- You can access the configuration utility from a Web browser if you know the IP address or host name of the access point.

---

**NOTE:** The default host name of the access point is **CEN-WAP-ABG-1G**.

---

For additional information, refer to “Using a Web Browser” on page 16.

- You can access the configuration utility from the Crestron Toolbox if the access point is configured to operate in DHCP mode (default configuration). The Crestron ToolBox automatically discovers the IP address of the access point. For additional information, refer to “Using the Crestron ToolBox” on page 16.

### ***Using a Web Browser***

To access the configuration utility from a Web browser:

1. Start your Web browser.
2. Go to the IP address or host name of the access point.

---

**NOTE:** If the default Web management port number of 80 has been changed, you must append the port number to the IP address by entering a colon followed by the new port number. If, for example, the IP address is 192.168.10.225 and the Web management port number has been changed from 80 to 150, go to **http://192.168.10.225:150**.

For information about changing the Web management port number, refer to “Configuring External Control Settings” on page 40.

---

The user name and password window opens, allowing you to log in to the access point. For log-in information, refer to “Logging In to the Access Point” on page 17.

### ***Using the Crestron ToolBox***

---

**NOTE:** To be able to use the Crestron Toolbox to access the configuration utility of the access point, the UPnP (Universal Plug and Play) Ethernet protocol configuration setting of the access point must be enabled. The UPnP protocol is enabled by default. For additional information, refer to “Configuring External Control Settings” on page 40.

---

To access the configuration utility from the Crestron Toolbox:

1. Open the Crestron Toolbox.
2. From the **Tools** menu, select **Device Discovery Tool**.

---

**NOTE:** You can also access the Device Discovery Tool by clicking the Device Discovery Tool button () in the toolbar.

**NOTE:** The security software running on your computer may send you a program alert regarding the attempt of Crestron Toolbox to connect to the network. You must allow the connection so that the Device Discovery tool can be used.

---

3. From the device list on the left-hand side of the screen, select the UPnP name of the access point. The default UPnP name is **CEN-WAP-ABG-1G**.

The user name and password window opens, allowing you to log in to the access point. For log-in information, refer to “Logging In to the Access Point” on page 17.

## Logging In to the Access Point

The user name and password window allows you to log in to the access point.

### “User Name and Password” Window



To log in to the access point:

1. Enter the user name and password. The default user name is *admin*, and the default password is *admin*.

---

**NOTE:** The user name and password are *not* case sensitive.

**NOTE:** For enhanced security, it is recommended that you change the default user name and password. For information about changing the user name and password, refer to “Configuring User Name and Password Settings” on page 37.

---

2. Click **OK**. The Home page of the access point opens, allowing you to select the desired configuration mode. Refer to “Selecting the Configuration Mode” below for information.

## Selecting the Configuration Mode

The Home page allows you to select the desired configuration mode.

### CEN-WAP-ABG Home Page



To select the configuration mode, do either of the following:

- Click **Setup Wizard** if you wish to configure the access point using the wizard. Refer to “Using Setup Wizard Configuration Mode” below for detailed information.
- Click **Custom Settings** if you wish to customize the settings of the access point. Refer to “Using Custom Settings Configuration Mode” on page 20 for detailed information.

## Using Setup Wizard Configuration Mode

Setup Wizard configuration mode provides automated access to the screens necessary to set any of the following configuration profiles:

- **802.11b/g:** Provides wireless access to all Crestron Wi-Fi touchpanels, such as the TPMC-4X, TPMC-4XG, TPMC-8, and TPMC-10. The 802.11b/g configuration profile also provides wireless access to third-party wireless devices.
- **802.11a:** Provides wireless access to 802.11a-enabled Crestron Wi-Fi touchpanels such as the TPMC-8X.

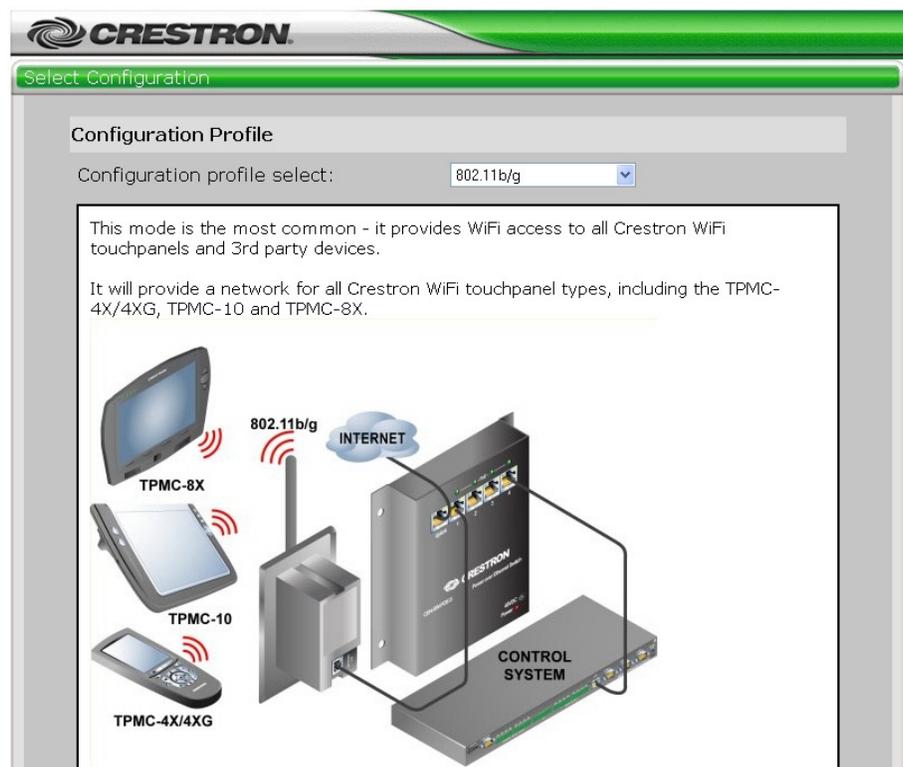
---

**NOTE:** The 802.11a configuration profile provides better reliability than 802.11b/g but slightly less range. If your installation has many wireless networks nearby or has sources of interference such as microwaves or 2.4 GHz cordless phones, 802.11a may provide a more robust solution than 802.11b/g.

---

- **High Security TPMC-8X:** Provides an extremely high level of network and physical security for corporate environments. Because of the required security features, this configuration profile provides wireless access to the TPMC-8X only.
- **Standalone Network:** Applicable only when the Crestron network is not connected to an Ethernet network. This configuration profile enables the access point to function as a DHCP server and provide IP addresses to Ethernet equipment.

To access Setup Wizard configuration mode, open the Home page and click **Setup Wizard**. The “Select Configuration” page opens.

*“Select Configuration” Page (802.11b/g Configuration Profile Shown)*

To use the wizard:

1. On the “Select Configuration” page, select a configuration profile (**802.11b/g, 802.11a, High Security TPMC-8X, or Standalone Network**). For detailed information about each of the configuration profiles, read the information provided in the setup wizard for each profile.
2. Click **Next**. The “Network Setting” page opens, displaying the network name, which is also referred to as the SSID (service set identifier) of the access point.

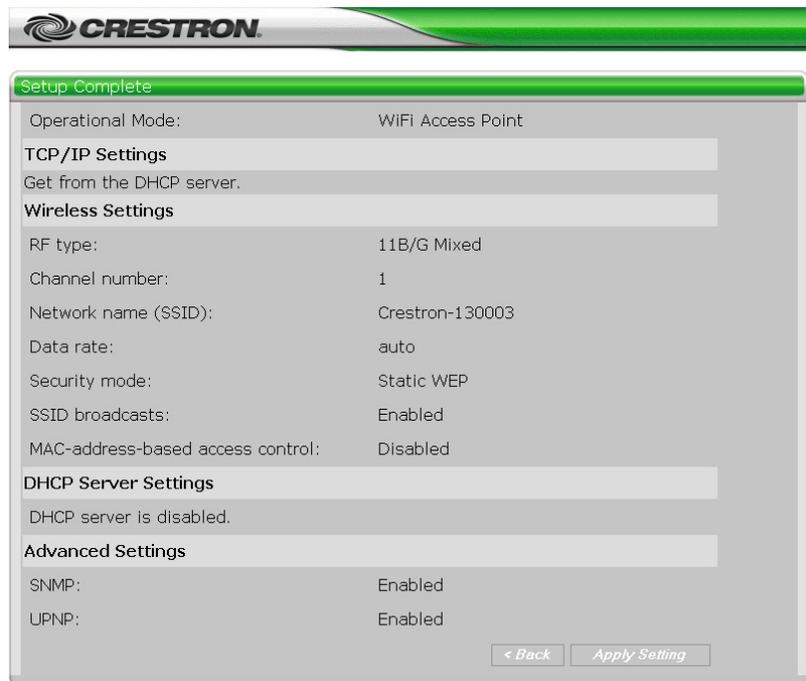
*“Network Setting” Page*

3. In the *Select Passkey* text box, enter a network key.

**NOTE:** The network key is case sensitive. Permissible characters are 0 to 9, a to f, and A to F. If the configuration profile is **802.11b/g, 802.11a, or Standalone Network**, the network key must consist of 10 characters exactly. If the configuration profile is **High Security TPMC-8x**, the network key must consist of a minimum of 8 characters.

- Click **Next**. The “Setup Complete” page opens as shown in the following example.

*“Setup Complete” Page (802.11b/g Configuration Profile Shown)*



- Review the settings and, if appropriate for your wireless network, click **Apply Setting**. (If not appropriate, go back to the “Select Configuration” page and select a different configuration profile.)

---

**NOTE:** When you click **Apply Setting**, the “Setup Complete” page opens. The access point restarts to allow the settings to take effect (about 25 seconds).

---

- Connect your touchpanel to the access point by clicking the appropriate touchpanel (for example, TPMC-8X, TPMC-4X, or TPMC-10) and by following the on-screen instructions provided by the wizard. If your touchpanel is not listed, refer to the manual included with the touchpanel for instructions to connect the touchpanel to the access point.

## Using Custom Settings Configuration Mode

Custom Settings configuration mode allows you to do the following:

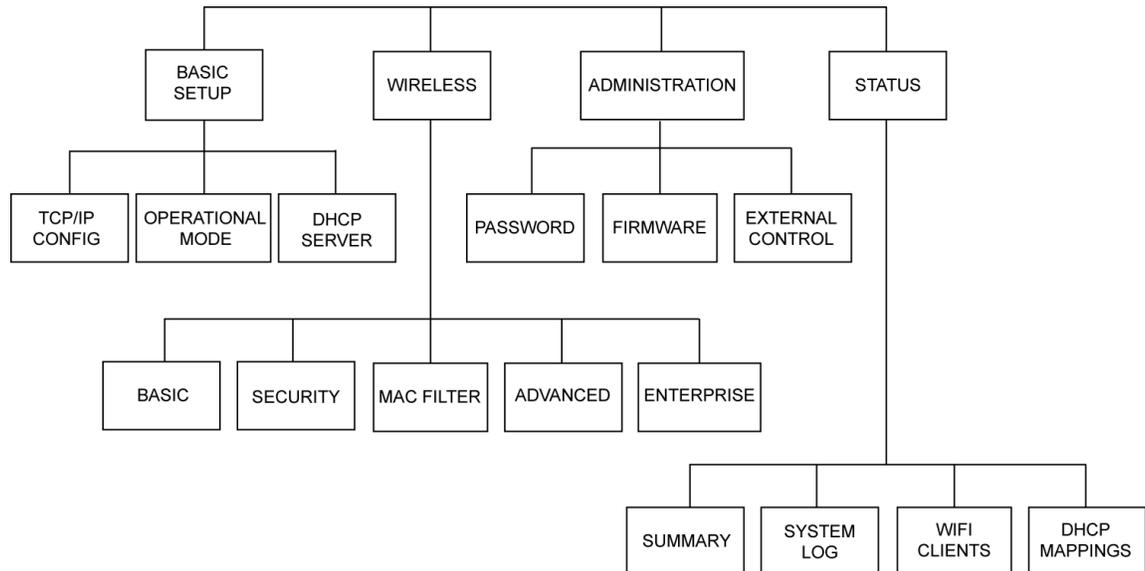
- Configure basic setup settings
- Configure wireless network settings
- Configure administrative settings
- View and monitor operational status

To access Custom Settings configuration mode, open the Home page and click **Custom Settings**.

## Navigating Custom Settings Configuration Mode

Custom Settings configuration mode provides four main tabs: *BASIC SETUP*, *WIRELESS*, *ADMINISTRATION*, and *STATUS*. The *BASIC SETUP*, *WIRELESS*, and *ADMINISTRATION* tabs provide subtabs that allow access to configuration pages. The *STATUS* tab provides subtabs that allow access to status pages. The following illustration demonstrates the menu tree of Custom Settings configuration mode.

*Custom Settings Menu Tree*



Note the following:

- For information about configuration pages accessed from the *BASIC SETUP* tab, refer to “Configuring Basic Setup Settings” on page 22.
- For information about configuration pages accessed from the *WIRELESS* tab, refer to “Configuring Wireless Settings” on page 27.
- For information about configuration pages accessed from the *ADMINISTRATION* tab, refer to “Configuring Administration Settings” on page 37.
- For information about status pages accessed from the *STATUS* tab, refer to “Viewing the Status of the Access Point” on page 42.

## Saving/Canceling Configuration Changes

To save changes that you make to a configuration page, click **Save settings** at the bottom of the page. If you do not wish to save your changes, click **Cancel**.

*Save Settings and Cancel Buttons*




---

**NOTE:** When you click **Save settings**, the access point saves the changes and restarts to allow the changes to take effect. After 15-20 seconds, the “Bridge AP Settings and Info” page opens to allow you to review the settings.

---

## Configuring Basic Setup Settings

Basic setup settings allow you to configure the following:

- TCP/IP addressing
- Operational mode
- DHCP server settings

### Configuring TCP/IP Addressing

To configure TCP/IP addressing, click the *BASIC SETUP* tab and then click the *TCP/IP CONFIG* subtab. The “TCP/IP Addressing” page opens.

#### “TCP/IP Addressing” Page

The screenshot shows the Crestron web interface for configuring TCP/IP settings. The main navigation bar includes 'BASIC SETUP', 'WIRELESS', 'ADMINISTRATION', and 'STATUS'. The 'BASIC SETUP' tab is active, and the 'TCP/IP CONFIG' sub-tab is selected. The 'TCP/IP Addressing' window contains the following fields:

- Connection type: Automatic Configuration - DHCP (dropdown menu)
- IP address: 192.168.100.1
- Subnet mask: 255.255.255.0
- Default router: 192.168.100.254
- Hostname: CEN-WAP-ABG-10
- Domain name: (empty text box)

Buttons for 'Save settings' and 'Cancel' are located at the bottom right of the form.

Refer to the configuration guidelines that follow.

*Connection type:* From the drop-down list, select either of the following:

- **Automatic Configuration – DHCP:** (Default setting) Allows the IP address of the access point to be automatically assigned by a DHCP (Dynamic Host Configuration Protocol) server on the local area network (LAN) for a predetermined period of time.
- **Static IP:** Allows you to manually set a permanent IP address for the access point as well as additional settings:

*IP address:* Enter a unique IP address for the access point.

*Subnet mask:* Enter the subnet mask that is set on your network.

---

**NOTE:** A class C network allows up to 255 devices to communicate without a router and has a subnet mask of 255.255.255.0. A class B network allows up to 65,535 devices to communicate without a router and has a subnet mask of 255.255.0.0.

---

*Default router:* Enter the IP address of your network’s device (usually a router) that enables communication between your network and the Internet.

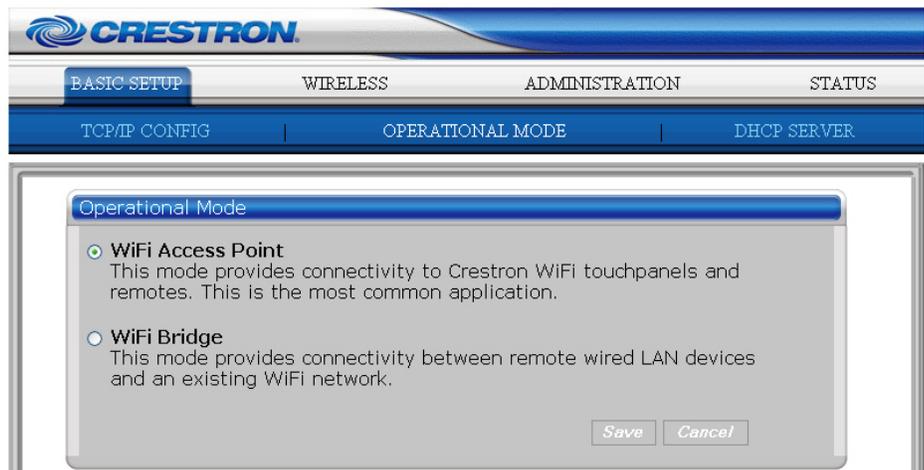
*Hostname:* (Optional) Enter a name that identifies the access point on the network. The hostname is restricted to the letters *a* to *z* (not case sensitive), the digits *1* to *9*, and the hyphen. The default setting is **CEN-WAP-ABG-1G**.

*Domain name:* (Optional) Enter a domain name for the access point.

#### Configuring Operational Mode

To configure operational mode, click the *BASIC SETUP* tab and then click the *OPERATIONAL MODE* subtab. The “Operational Mode” page opens.

#### “Operational Mode” Page



Refer to the configuration guideline that follows.

Click either of the following radio buttons:

- **WiFi Access Point:** (Default setting) Provides connectivity to Crestron Wi-Fi touchpanels and remote controls.
- **WiFi Bridge:** Provides connectivity between remote wired LAN devices and an existing Wi-Fi network.

#### Configuring DHCP Server Settings

If a DHCP server does not exist on the network, the access point can be configured as a DHCP server to automatically assign IP addresses to client devices on the network.

---

**NOTE:** An IP address is leased by the access point to a client device for 24 hours.

---

To configure the access point as the DHCP server in your network, click the *BASIC SETUP* tab and then click the *DHCP SERVER* subtab. The “DHCP Server” page opens.

*“DHCP Server” Page (DHCP Disabled)*

The screenshot shows the DHCP Server configuration page. At the top, there is a navigation bar with tabs for BASIC SETUP, WIRELESS, ADMINISTRATION, and STATUS. Below this, there are sub-tabs for TCP/IP CONFIG, OPERATIONAL MODE, and DHCP SERVER. The main content area is titled 'DHCP Server' and contains a 'Basic' section. In the 'Basic' section, the 'Functionality' is set to 'Disable' in a drop-down menu. Below this is a section for 'Static DHCP Mappings' which contains a table with the following columns: Enabled, Desc., MAC Address, and IP Address. The table has eight rows, each with an unchecked checkbox in the 'Enabled' column and empty input fields for the other columns.

Refer to the configuration guidelines that follow.

*Functionality:* From the drop-down list, select either of the following:

- **Disable:** (Default setting) Prevents the access point from functioning as a DHCP server. Select **Disable** if you do not want a DHCP server or if you already have a DHCP server (such as a router) on your network.
- **Enable:** Allows the access point to function as a DHCP server. Select **Enable** if your network has a switch instead of a router.

---

**NOTE:** Only one DHCP server can exist on your network. Multiple DHCP servers on the same network cause network issues.

---

If you have enabled the access point to function as a DHCP server, configure DHCP server settings as follows.

**Basic DHCP server configuration:** The following shows the *Basic* section of the “DHCP Server” page when DHCP server functionality is enabled in the *Functionality* drop-down list.

*“DHCP Server” Page – Basic (DHCP Enabled)*

Field	Value
Functionality	Enable
Default gateway	192.168.100.1
Subnet mask	255.255.255.0
Primary DNS server	192.168.100.1
Secondary DNS server	192.168.100.10
Starting IP address	192.168.100.100
Maximum number of DHCP users	100

*Default gateway:* Enter the IP address of the access point, which is to be used as your network’s gateway. The default gateway address is provided to all client devices that request an IP address from the access point via DHCP. The default setting is **192.168.100.1**.

*Subnet mask:* Enter the subnet mask that is set on your network. The subnet mask is provided to all client devices that request an IP address from the access point via DHCP. The default setting is **255.255.255.0**.

---

**NOTE:** A class C network allows up to 255 devices to communicate without a router and has a subnet mask of 255.255.255.0. A class B network allows up to 65,535 devices to communicate without a router and has a subnet mask of 255.255.0.0.

---

*Primary DNS server:* Enter the IP address of the primary DNS server. The primary DNS server address is provided to all client devices that request an IP address from the access point via DHCP. The default setting is **192.168.100.1**.

*Secondary DNS server:* Enter the IP address of the secondary DNS server. The secondary DNS server address is provided to all client devices that request an IP address from the access point via DHCP. The default setting is **192.168.100.10**.

*Starting IP address:* Enter the first IP address to be assigned to a client device by the access point. The default setting is **192.168.100.100**.

*Maximum number of DHCP users:* Enter the maximum number of client devices to which the access point can assign IP addresses. The default setting is **100**.

---

**NOTE:** The maximum number of DHCP users is 253, which is possible only if the IP address of the access point is 192.168.1.1 and the starting IP address is 192.168.1.2.

---

**Static DHCP Mappings configuration:** The following shows the *Static DHCP Mappings* section of the “DHCP Server” page.

**“DHCP Server” Page – Static DHCP Mappings**

Enabled	Desc.	MAC Address	IP Address
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

The *Static DHCP Mappings* section allows you to assign static IP addresses to DHCP client devices. As a result, a client device is always assigned the same IP address by the access point. Static DHCP mappings provide the advantage of a static IP setup and allow configuration of IP addresses from a single point.

To assign a static IP address to a client device:

1. Click the *Enabled* checkbox. (To disable the mapping, click the checkbox again to remove the checkmark.)
2. In the *Desc.* column, enter a description for the mapping.
3. In the *MAC address* column, enter the MAC address of the client device in the format **xx-xx-xx-xx-xx-xx**.
4. In the *IP Address* column, enter the IP address to be assigned to the client device.

Examples of static DHCP mappings follow.

*Static DHCP Mapping Examples*

Static DHCP Mappings 

Enabled	Desc.	MAC Address	IP Address
<input checked="" type="checkbox"/>	Bill	00-90-4B-00-89-BD	192.168.168.214
<input checked="" type="checkbox"/>	John	00-BB-DE-AD-BE-EF	192.168.168.224
<input checked="" type="checkbox"/>	Jeff	00-90-4B-00-40-94	192.168.168.226
<input checked="" type="checkbox"/>	Tom	00-40-01-43-1D-E8	192.168.168.230
<input type="checkbox"/>			

**Configuring Wireless Settings**

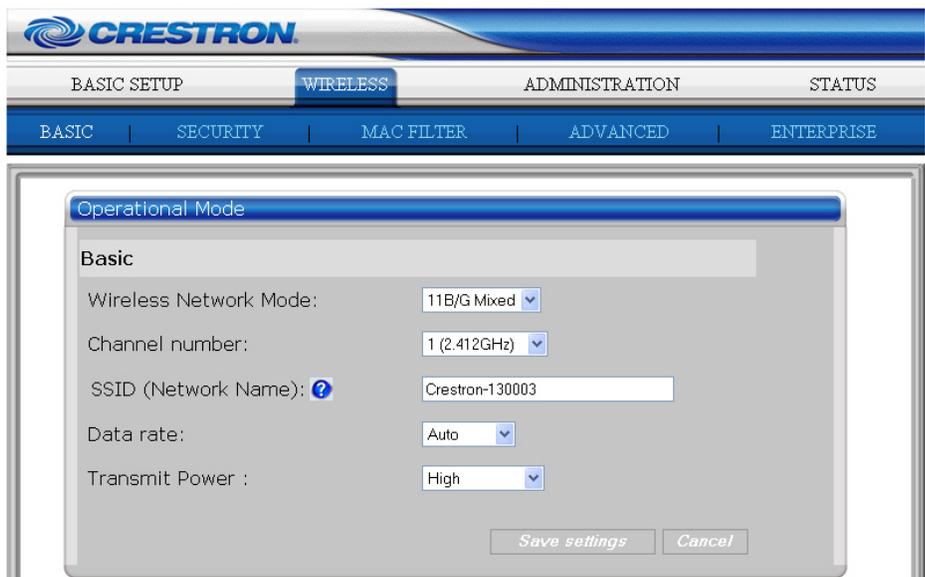
Wireless settings allow you to configure the following:

- Basic wireless settings
- IEEE 802.11 security settings
- MAC filters
- Advanced wireless settings
- Enterprise (IEEE 802.1x/RADIUS) settings

**Configuring Basic Wireless Settings**

To configure basic wireless settings, click the *WIRELESS* tab and then click the *BASIC* subtab. The “Operational Mode” page opens.

*“Operational Mode” Page (Wireless)*



Refer to the configuration guidelines that follow.

*Wireless Network Mode:* From the drop-down list, select one of the following IEEE wireless standard options:

- **11B Only:** Specifies 802.11b, which allows a maximum data transfer rate of 11 Mbps and an operating frequency of 2.4 GHz.
- **11G Only:** Specifies 802.11g, which allows a maximum data transfer rate of 54 Mbps and an operating frequency of 2.4 GHz.
- **11 B/G Mixed:** (Default setting) Specifies both 802.11b and 802.11g.

---

**NOTE:** The presence of a single 802.11b client device forces all devices to operate using 802.11b instead of 802.11g.

---

- **11A:** Specifies 802.11a, which allows a maximum data transfer rate of 54 Mbps and an operating frequency of 5 GHz.

*Channel number:* From the drop-down list, do either of the following:

- Select **Auto** to allow the access point to automatically select an RF channel based on other channels already in use. The access point looks at nearby access points in the channel range 1-11 and selects the first available channel that has no other networks present.
- Select the appropriate RF channel for your wireless network. Channel numbers range from **1 (2.412 GHz)** (default setting) to **11 (2.462 GHz)**.

---

**NOTE:** The number of available RF channels depends on local regulations.

**NOTE:** To avoid one access point from interfering with others in range, set the channel number of the access points to different channels. In 802.11b networks, use channels 1, 6, and 11 to ensure enough frequency separation to avoid conflicts. For additional information, refer to the latest version of the Best Practices for Installation and Setup of Crestron RF Products Reference Guide (Doc. 6689), which is available for download from the Crestron website.

---

*SSID (Network Name):* Enter a unique name (service set identifier) for the wireless network. The SSID is used by all wireless clients to connect to the access point. The default setting is unique for each access point and is named **Crestron-xxxxxx**, where **xxxxxx** represents the last three octets of the MAC address.

*Data rate:* From the drop-down list, do either of the following:

- Select **Auto** (default setting) to allow the access point to automatically use the fastest possible data rate.
- Select the appropriate rate of data transmission based on the speed of your wireless network. The data rate ranges from **1 Mbps** to **54 Mbps**.

---

**NOTE:** The recommended setting is **Auto**. If, however, RF interference exists, reduce the data rate for more reliable wireless transmission.

---

*Transmit Power:* From the drop-down list, select the desired level of transmit power to change the RF coverage: **High** (default setting), **Medium High**, **Medium**, **Medium Low**, or **Low**.

Setting the transmit power to the highest level maximizes the range, which reduces the number of access points necessary. If you wish to increase the capacity of the network by placing access points closer together, set the transmit power to a lower value to decrease overlap. In addition, lower power settings improve security by limiting wireless signals from propagating outside the physically controlled area of the site.

### Configuring IEEE 802.11 Security Settings

To configure IEEE 802.11 security settings, click the *WIRELESS* tab and then click the *SECURITY* subtab. The “IEEE 802.11 Security” page opens.

#### “IEEE 802.11 Security” Page

The screenshot displays the 'IEEE 802.11 Security' configuration page. At the top, there is a navigation bar with tabs for 'BASIC SETUP', 'WIRELESS', 'ADMINISTRATION', and 'STATUS'. Below this, a sub-navigation bar includes 'BASIC', 'SECURITY', 'MAC FILTER', 'ADVANCED', and 'ENTERPRISE'. The main content area is titled 'IEEE 802.11 Security' and contains a 'Basic' section with the following settings:

- Wireless SSID broadcast: Enable
- Wireless client isolation: Disable
- Security mode: Static WEP
- Network Authentication: Open System
- Key length: 64 Bits
- Selected key: Key 1
- Key 1: [Masked]
- Key 2: [Masked]
- Key 3: [Masked]
- Key 4: [Masked]

Refer to the configuration guidelines that follow.

*Wireless SSID broadcast:* From the drop-down list, select either of the following:

- **Disable:** Prevents the access point from broadcasting the SSID to all wireless devices that are in range but not already associated with the network. Selecting **Disable** increases network security; however, new devices will not automatically discover the network and will require that the SSID be entered manually.
- **Enable:** (Default setting) Allows the access point to broadcast the SSID to all wireless devices.

*Wireless client isolation:* From the drop-down list, select either of the following:

- **Disable:** (Default setting) Allows wireless devices connected to the access point to communicate with one another.
- **Enable:** Prevents wireless devices connected to the access point from communicating with one another but allows communication with wired LAN devices.

*Security mode:* From the drop-down list, select the desired security mode:

- **Disable**

---

**NOTE:** Disabling wireless security is not recommended unless you experience wireless network connection problems.

**NOTE:** If you select **Disable**, it is recommended that you configure a wireless MAC filter to permit only authorized devices to connect to the network. To configure a wireless MAC filter, refer to “Configuring MAC Filters” on page 33.

---

- **Static WEP** (Wired Equivalent Privacy), default setting. Static WEP provides compatibility with all wireless devices and maintains as quick a reconnect time as when security is disabled.

---

**NOTE:** WEP keys must be manually configured.

---

- **Enterprise WEP**

---

**NOTE:** Enterprise WEP does not provide network authentication. As a result, any device can connect to the wireless network.

---

- **WPA-PSK with TKIP** (Wi-Fi Protected Access–Pre-Shared Key with Temporal Key Integrity Protocol)  
or  
**WPA-PSK with AES** (Wi-Fi Protected Access–Pre-Shared Key with Advanced Encryption Standard)

---

**NOTE:** WPA is supported by certain Crestron touchpanels only. For a particular touchpanel, refer to the operations guide and firmware release notes for information about supported wireless security modes.

---

- **WPA2-PSK with TKIP**  
or  
**WPA2-PSK with AES**

---

**NOTE:** WPA2 is supported by certain Crestron touchpanels only. For a particular touchpanel, refer to the operations guide and firmware release notes for information about supported wireless security modes.

---

- **Enterprise WPA with TKIP**  
or  
**Enterprise WPA with AES**

---

**NOTE:** Enterprise WPA requires a separate RADIUS (Remote Authentication Dial-In User Service) server to manage the log-in process and network keys. For information about configuring RADIUS settings, refer to “Configuring Enterprise (IEEE 802.1x/RADIUS) Settings” on page 35.

Enterprise WPA is the recommended security mode for secure corporate use.

---

- **Enterprise WPA2 with TKIP**  
or  
**Enterprise WPA2 with AES**

---

**NOTE:** Enterprise WPA2 requires a separate RADIUS (Remote Authentication Dial-In User Service) server to manage the log-in process and network keys. For information about configuring RADIUS settings, refer to “Configuring Enterprise (IEEE 802.1x/RADIUS) Settings” on page 35.

**NOTE:** Enterprise WPA2 is supported by certain Crestron touchpanels only. For a particular touchpanel, refer to the operations guide and firmware release notes for information about supported wireless security modes.

---

*Network Authentication:* (Applicable only to Static WEP security mode) From the drop-down list, select either of the following:

- **Open System:** (Default setting) Prevents authentication and data encryption. The sender and the recipient do not share a WEP key for authentication.
- **Shared Key:** The sender and the recipient share a WEP key for authentication.

---

**NOTE:** All devices on your network must use the same network authentication method.

---

*Key length:* (Applicable only to Static WEP and Enterprise WEP security modes) From the drop-down list, select **64 Bits** (default setting), **128 Bits**, or **152 Bits** (Static WEP only) as the level of WEP encryption. By selecting larger keys, the security level is raised and the length of the network key increases.

*Selected key:* (Applicable only to Static WEP security mode) From the drop-down list, select **Key 1**, **Key 2**, **Key 3**, or **Key 4** to be used as the key to encrypt data sent from the access point to a wireless client.

---

**NOTE:** All four keys decrypt data that is sent from a wireless client to the access point.

---

*Key 1 - Key 4:* (Applicable only to Static WEP security mode) For each key, enter hexadecimal characters. Valid hexadecimal characters are 0 to 9, a to f, and A to F (the string of characters is *not* case sensitive):

- If you selected **64 Bits** as the *Key length*, enter 10 hexadecimal characters.
- If you selected **128 Bits** as the *Key length*, enter 26 hexadecimal characters.
- If you selected **152 Bits** as the *Key length*, enter 32 hexadecimal characters.

*Network Key:* (Applicable only to WPA-PSK and WPA2-PSK with TKIP or AES security modes) Enter a network key from 8-32 characters (case sensitive). The network key is used as a master key to automatically generate keys that encrypt outgoing data and decrypt incoming data. The network key must be the same for all wireless devices connected to a network using WPA-PSK/WPA2-PSK security.

---

**NOTE:** The network key is also referred to as a pre-shared key (PSK) or passphrase.

---

### Configuring Advanced Wireless Settings

To configure advanced wireless settings, click the *WIRELESS* tab and then click the *ADVANCED* subtab. The “Advanced” page opens.

#### “Advanced” Page

The screenshot shows the Crestron configuration web interface. At the top is the Crestron logo. Below it is a navigation bar with tabs for 'BASIC SETUP', 'WIRELESS', 'ADMINISTRATION', and 'STATUS'. Under the 'WIRELESS' tab, there are sub-tabs for 'BASIC', 'SECURITY', 'MAC FILTER', 'ADVANCED', and 'ENTERPRISE'. The 'ADVANCED' sub-tab is selected, and a dialog box titled 'Advanced' is open. This dialog contains the following settings:

Frag. Threshold (byte): ?	<input type="text" value="2346"/>
RTS Threshold (byte): ?	<input type="text" value="2346"/>
Beacon Interval (ms): ?	<input type="text" value="100"/>
DTIM: ?	<input type="text" value="1"/>

At the bottom right of the dialog are two buttons: 'Save settings' and 'Cancel'.

Refer to the configuration guidelines that follow.

*Frag. Threshold (byte):* In the text box, enter the maximum number of bytes a data packet must be before breaking into smaller pieces (fragmenting) and transmitting over the network. The default setting is **2346**.

---

**NOTE:** The recommended setting is 2346 bytes (default). A smaller setting creates smaller packets and therefore more packets for each transmission. In areas, however, where wireless communication is poor or a great deal of radio interference occurs, you may lower the setting to about 500 bytes.

**NOTE:** Whenever you change the default setting, it is recommended that you perform range and reconnection testing.

---

*RTS Threshold (byte):* In the text box, enter the maximum number of bytes a data packet must be before the access point can issue a request to send (RTS). The default setting is **2346**.

---

**NOTE:** A low value causes RTS packets to be sent more often, consuming more of the available bandwidth and therefore reducing the apparent throughput of the network packet. The more packets that are sent, however, the quicker the access point can recover from interference or collisions.

If several touchpanels are connected to a single access point, lowering the RTS threshold to a value ranging from 500 to 1000 may improve performance. Assigning a dedicated access point to each touchpanel improves the performance more.

---

*Beacon Interval (ms):* In the text box, enter the desired number of milliseconds between beacon transmissions. The access point transmits beacons to let the wireless clients know its name and information. The default setting is **100**.

---

**NOTE:** By increasing the beacon interval, you reduce the number of beacons and associated overhead. Increasing the beacon interval, however, delays the association and roaming process since devices scanning for available access points may miss the beacons.

A high value ranging from 250 to 500 milliseconds may improve performance in areas with high radio interference but can also increase reconnection time. Decreasing the value below 100 does not improve reconnection time.

---

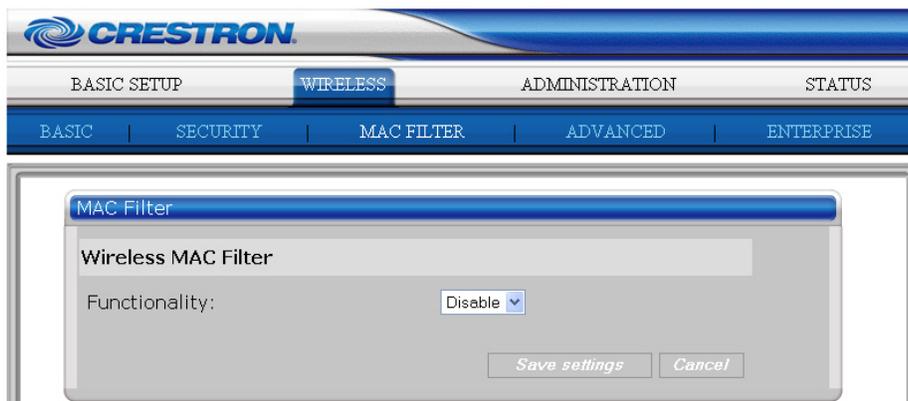
*DTIM:* Delivery Traffic Indication Message (not currently supported by Crestron Wi-Fi devices)

### Configuring MAC Filters

MAC filters allows you to prevent or permit access to the wireless network from wireless computers with specific MAC addresses.

To configure MAC filters, click the *WIRELESS* tab and then click the *MAC FILTER* subtab. The “MAC Filter” page opens.

#### “MAC Filter” Page (MAC Filtering Disabled)



Refer to the configuration guidelines that follow.

*Functionality:* From the drop-down list, select either of the following:

- **Disable:** Prevents MAC address filtering.
- **Enable:** (Default setting) Allows MAC address filtering.

The following shows the “MAC Filter” page when MAC filtering is enabled in the *Functionality* drop-down list.

*“MAC Filter” Page (MAC Filtering Enabled)*

The screenshot shows the Crestron web interface for the MAC Filter configuration. The navigation menu includes BASIC SETUP, WIRELESS (selected), ADMINISTRATION, and STATUS. Below this, there are sub-menus for BASIC, SECURITY, MAC FILTER (selected), ADVANCED, and ENTERPRISE. The main content area is titled 'MAC Filter' and contains the following sections:

- Wireless MAC Filter:**
  - Functionality: Enable (dropdown)
  - Access control type: Permit only (dropdown)
  - MAC Address: [input field] Add
  - MAC address format: 00:02:DD:30:03:1E
  - Table with columns: No., MAC Address, Delete
- MAC Filter List Download:**
  - MAC Filter List Filename: [input field] Browse...
  - Upload

If you have enabled MAC filtering, configure MAC filter settings as follows.

*Access control type:* In the drop-down list, select either of the following:

- **Prevent:** Denies wireless network access to up to 64 specific wireless devices.
- **Permit only:** (Default setting) Permits wireless network access to up to 64 specific wireless devices.

Specify MAC addresses of a maximum of 64 wireless devices whose access you want to control by doing either of the following:

- Manually enter MAC addresses one at a time:

In the *MAC Address* text box, enter a MAC address in hexadecimal format (**xx-xx-xx-xx-xx-xx**), and then click **Add**. The MAC address appears at the bottom of the MAC filter list.

Up to 64 MAC addresses can be added to the list – one address at a time.

- Download a MAC filter list to the access point:
  1. Prepare a text file containing a maximum of 64 MAC addresses, and save the file in the desired location. A sample of a text file follows.

**Sample MAC Address Text File**

```
00-11-22-33-44-50
00-11-22-33-44-51
00-11-22-33-44-52
00-11-22-33-44-53
00-11-22-33-44-54
00-11-22-33-44-55
00-11-22-33-44-56
00-11-22-33-44-57
00-11-22-33-44-58
00-11-22-33-44-59
00-11-22-33-44-5a
00-11-22-33-44-5b
00-11-22-33-44-5c
00-11-22-33-44-5d
00-11-22-33-44-5e
00-11-22-33-44-5f
```

2. In the *MAC Filter List Filename* text box, enter the path of the text file or click **Browse** to locate the file.
3. Click **Upload** to upload the text file to the access point.

A message appears indicating that the procedure for firmware upgrading takes about 1-2 minutes. The MAC addresses in the text file appear in the MAC filter list.

---

**NOTE:** To remove a MAC address from the MAC filter list, click **Delete**.

---

**Configuring Enterprise  
(IEEE 802.1x/RADIUS)  
Settings**

---

**NOTE:** Configure Enterprise settings only if you plan to use a RADIUS server in conjunction with the access point for authentication and only if wireless security mode is set to any of the following: **Enterprise WPA with TKIP**, **Enterprise WPA with AES**, **Enterprise WPA2 with TKIP**, or **Enterprise WPA2 with AES**.

---

To configure IEEE 802.1x/RADIUS settings, click the *WIRELESS* tab and then click the *ENTERPRISE* subtab. The “IEEE 802.1x/RADIUS” page opens.

*“IEEE 802.1x/RADIUS” Page*

The screenshot shows the "IEEE 802.1x/RADIUS" configuration page. The navigation menu includes BASIC SETUP, WIRELESS (selected), ADMINISTRATION, and STATUS. Below this are sub-menus: BASIC, SECURITY, MAC FILTER, ADVANCED, and ENTERPRISE. The main configuration area contains the following fields:

- Primary RADIUS server address: 192.168.0.220
- Secondary RADIUS server address: (empty)
- Timeout (sec): 5
- Max number of retries: 3
- RADIUS authentication port: 1812
- RADIUS accounting port: 1813
- Shared key: (masked with dots)
- Network Access Server (NAS) identifier: Crestron

Buttons for "Save settings" and "Cancel" are located at the bottom right of the configuration area.

Refer to the configuration guidelines that follow.

*Primary RADIUS server address:* Enter the IP address of the primary RADIUS server.

---

**NOTE:** The access point can be configured to communicate with two RADIUS servers: a primary server and a secondary server. If the primary RADIUS server fails to respond, the access point can try to communicate with the secondary RADIUS server.

---

*Secondary RADIUS server address:* Enter the IP address of the secondary RADIUS server.

*Timeout (sec):* Enter the maximum number of seconds that must pass before the access point can try to communicate with the secondary RADIUS server after failing to communicate with the primary RADIUS server. The default setting is **5**.

*Max number of retries:* Enter the maximum number of times the access point can try to communicate with the primary RADIUS server after the initial attempt fails. When the maximum number of retries is reached and communication with the primary RADIUS server fails, the access point can try to communicate with the secondary RADIUS server. The default setting is **3**.

*RADIUS authentication port:* Enter the authentication port number of the RADIUS server. The default setting is **1812**.

---

**NOTE:** The RADIUS authentication port is officially assigned to UDP port 1812. RADIUS servers of Microsoft Corporation default to port 1812; however, RADIUS servers of Juniper Networks, Inc. and Cisco Systems, Inc. default to port 1645.

---

*RADIUS accounting port:* Enter the accounting port number of the RADIUS server. The default setting is **1813**.

**NOTE:** The RADIUS accounting port is officially assigned to UDP port 1813. RADIUS servers of Microsoft Corporation default to port 1813; however, RADIUS servers of Juniper Networks, Inc. and Cisco Systems, Inc. default to port 1646.

*Shared key:* Enter a secret key to be shared by the access point and the RADIUS server so that they can authenticate each other. Valid characters are 0 to 9, a to f, and A to F. Note that the shared key is case sensitive.

*Network Access Server (NAS) Identifier:* Enter a unique NAS identifier to identify the access point in addition to its IP address. The default setting is **Crestron**.

### **Configuring Administration Settings**

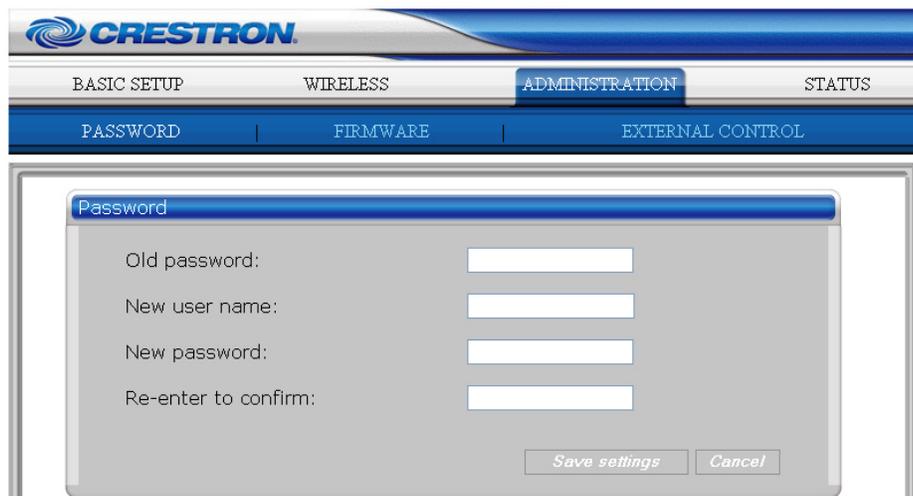
Administration settings allow you to do the following:

- Assign a new user name and password
- Upgrade the firmware of the access point
- Restore previous configuration settings of the access point
- Back up current configuration settings of the access point
- Restore factory default settings of the access point
- Configure external control settings (for example, enable or disable the front Ethernet port)

#### **Configuring User Name and Password Settings**

To configure user name and password settings, click the *ADMINISTRATION* tab and then click the *PASSWORD* subtab. The “Password” page opens.

#### **“Password” Page**



The screenshot displays the Crestron administration web interface. At the top, the Crestron logo is visible. Below it, a navigation bar contains tabs for BASIC SETUP, WIRELESS, ADMINISTRATION (which is selected), and STATUS. Under the ADMINISTRATION tab, there are sub-tabs for PASSWORD, FIRMWARE, and EXTERNAL CONTROL. The PASSWORD sub-tab is active, showing a form titled "Password" with the following fields: "Old password:", "New user name:", "New password:", and "Re-enter to confirm:". Each field has a corresponding text input box. At the bottom right of the form, there are two buttons: "Save settings" and "Cancel".

Refer to the configuration guidelines that follow.

---

**NOTE:** The user name and password are *not* case sensitive.

---

*Old password:* Enter the old password.

*New user name:* Enter a new user name.

*New password:* Enter a new password.

*Re-enter to confirm:* Reenter the new password for confirmation of the password.

### Upgrading Firmware

---

**NOTE:** Upgrading the firmware of the access point may cause a loss of the current configuration settings; therefore, be sure to back up the current configuration settings before upgrading the firmware. For information about backing up configuration settings, refer to “Backing Up Current Configuration Settings” on page 39.

---

To upgrade firmware of the access point, click the *ADMINISTRATION* tab and then click the *FIRMWARE* subtab. The “Firmware Tools” page opens.

#### “Firmware Tools” Page – Firmware Upgrade



Refer to the configuration guidelines that follow.

*Please select a file to upgrade:* In the text box, enter the path to the filename containing the new firmware by clicking **Browse** and selecting the firmware file from the Crestron website.

---

**NOTE:** Before upgrading the firmware, be sure to read the release notes.

---

Click **Upgrade** to start the firmware upgrade process. The access point reboots automatically when the upgrade is complete.

### Restoring Previous Configuration Settings

If necessary, you can restore previous access point configuration settings from your computer’s hard drive.

To restore previous configuration settings, click the *ADMINISTRATION* tab and then click the *FIRMWARE* subtab. The “Firmware Tools” page opens.

#### “Firmware Tools” Page – Restore Configuration



Refer to the configuration guidelines that follow.

*Please select a file to restore:* In the text box, enter the path to the filename containing previous configuration settings by clicking **Browse** and selecting the configuration file from your computer's hard drive.

Click **Restore** to start the configuration restore process. The access point reboots automatically when the configuration restore process is complete.

### Backing Up Current Configuration Settings

You can back up the file containing current configuration settings of the access point to your computer's hard drive. The default configuration filename is config.bin.

To back up current configuration settings, click the *ADMINISTRATION* tab and then click the *FIRMWARE* subtab. The "Firmware Tools" page opens.

#### "Firmware Tools" Page – Backup Configuration



Back up the current configuration as follows:

1. Click **Back Up** to open the "File Download" window.
2. Click **Save** to open the "Save As" window.
3. Navigate to the location on your hard drive to which you want to save the configuration file.
4. (Optional) In the *File name* text box, enter a new file name if desired.
5. Click **Save** to open the "Download Complete" window and save the file.
6. When the download is complete, click **Close**.

You can then load the configuration file to any CEN-WAP-ABG access point by performing the configuration restore process discussed in "Restoring Previous Configuration Settings" on page 38.

### Restoring Factory Default Settings

To restore factory default configuration settings of the access point, click the *ADMINISTRATION* tab and then click the *FIRMWARE* subtab. The "Firmware Tools" page opens.

#### "Firmware Tools" Page – Restore Factory Defaults



Click **Reset** to restore factory default settings.

---

**NOTE:** The access point restarts to allow the factory default settings to take effect. After 15-20 seconds, the "Bridge/AP Settings and Info" page opens to allow you to review the settings.

---

**Configuring External Control Settings**

External control settings consist of the following:

- Basic security settings that include enabling/disabling the front Ethernet port and assigning a new Web management port number.
- UPnP (Universal Plug and Play) Ethernet protocol settings that allow autodiscovery of devices on the local network.
- SNMP (Simple Network Management Protocol) Ethernet protocol settings that allow a device to be administered remotely.

To configure external control settings, click the *ADMINISTRATION* tab and then click the *EXTERNAL CONTROL* subtab. The “External Control” page opens.

Refer to the configuration guidelines that follow.

**Basic external control configuration:** The following shows the *Basic* section of the “External Control” page.

**“External Control” Page – Basic**

**Front Ethernet Port:** From the drop-down list, select either of the following:

- **Disable:** Disables functionality of the port. Because the port is accessible from the front of the access point, this setting is recommended to enhance security when the device is installed in an insecure location.
- **Enable:** (Default setting) Enables functionality of the port.

**Web management port (default is 80):** Enter a value from **1** to **65535**. It is recommended that you change the default setting to enhance security.

**UPNP (Universal Plug and Play) configuration:** The following shows the *UPnP* section of the “External Control” page.

**“External Control” Page – UPnP**

From the drop-down list, select either of the following:

- **Disable:** Prevents the access point from transmitting UPnP broadcast messages and therefore increases device security on an insecure network.

---

**NOTE:** Disabling UPnP prevents the Device Discovery Tool of the Crestron Toolbox from finding the access point on the network. As a result, the configuration utility of the access point can only be accessed from a Web browser.

**NOTE:** Disabling UPnP does not affect communication between Crestron touchpanels and the control system.

---

- **Enable:** (Default setting) Allows the access point to transmit UPnP broadcast messages. As a result, the Device Discovery Tool of the Crestron Toolbox can find the access point on the network.

*UPnP Name:* (Applicable only when UPnP is enabled) In the text box, enter a name for the access point to distinguish it from other devices that appear in the device list of the Device Discovery Tool. The default setting is **CEN-WAP-ABG-1G**.

**SNMP (Simple Network Management Protocol) configuration:** The following shows the *SNMP* section of the “External Control” page.

**“External Control” Page – SNMP**

From the drop-down list, select either of the following:

- **Disable:** Prevents the access point from being administered remotely via SNMP.
- **Enable:** (Default setting) Allows the access point to be administered remotely via SNMP.

Assign read-only or read-write privileges to the SNMP manager (applicable only if SNMP is enabled):

*Read-only community:* In the text box, enter a text string that functions as a password to allow the SNMP manager to read configuration settings from the access point. The default setting is **public**. The read-only community text string appears as solid black circles.

*Read-write community:* In the text box, enter a text string that functions as a password to allow the SNMP manager to read configuration settings from and write configuration settings to the access point. The default setting is **private**. The read-write community text string appears as solid black circles.

**SNMP Trap Table:** Add entries to the SNMP Trap Table to send notification events from the access point to SNMP managers when a significant event occurs:

1. Click the checkbox to activate trap notification.
2. In the *IP Address* column, enter the IP address of the device to which the access point is to send traps.
3. In the *Community* column, enter a read-only or read-write community text string.

### Viewing the Status of the Access Point

In addition to configuration of the access point, Custom Settings configuration mode allows you to view and monitor operational status of the access point. The access point displays the following information:

- A summary of configuration settings and general information
- The status of the wireless clients currently associated with the access point
- A log of system events
- A list of DHCP mappings

#### Viewing Summary Information

To view a summary of current configuration settings and general information, click the *STATUS* tab and then click the *SUMMARY* subtab. The “Bridge/AP Settings and Info” page opens.

**NOTE:** If one or more configuration settings appear in red, the access point must be restarted in order for the setting(s) to take effect. To restart the access point, press **Restart** at the bottom of the screen. After 15-20 seconds, the “Bridge AP Settings and Info” page opens again to allow you to review the settings.

**NOTE:** Since the “Bridge/AP Settings and Info” page displays the current settings and status of the access point, you can save or print the page for future reference.

The following shows the general information displayed by the “Bridge/AP Settings and Info” page.

#### “Bridge/AP Settings and Info” Page – General Information

CRESTRON	
BASIC SETUP	WIRELESS
ADMINISTRATION	
STATUS	
SUMMARY	SYSTEM LOG
WIFI CLIENTS	DHCP MAPPINGS
Bridge/AP Settings and Info	
Model:	CEN-WAP-ABG-1G
BIOS/Firmware version:	1.1.1.1/1.3.1.1
Operational Mode:	WiFi Access Point
MAC address:	00:10:7F:13:00:03
System up time (hr:min:sec)	28:59:51

*Model:* Displays the model number of the access point: **CEN-WAP-ABG-1G**.

*BIOS/Firmware version:* Displays the BIOS (Basic Input/Output System) and firmware versions.

*Operational Mode:* Displays the basic operational mode: **WiFi Access Point** or **WiFi Bridge**.

*MAC address:* Displays the MAC address of the access point.

*System up time (hr:min:sec):* Displays the amount of time in hours, minutes, and seconds that the access point has been powered on.

**TCP/IP Settings:** The following shows the *TCP/IP Settings* section of the “Bridge/AP Settings and Info” page.

**“Bridge/AP Settings and Info” Page – TCP/IP Settings**

TCP/IP Settings	
Get from the DHCP server.	
IP address:	172.30.16.29
Subnet mask:	255.255.255.0
Default gateway:	172.30.16.1

*IP address:* Displays the IP address of the access point.

*Subnet mask:* Displays the subnet mask of the network.

*Default gateway:* Displays the IP address of the default gateway.

**Wireless Settings:** The following shows the *Wireless Settings* section of the “Bridge/AP Settings and Info” page.

**“Bridge/AP Settings and Info” Page – Wireless Settings**

Wireless Settings	
Wireless Network Mode:	11B/G Mixed
Channel number:	1
Network name (SSID):	Crestron-130003
Data rate:	auto
Security mode:	Static WEP
SSID broadcasts:	Enable
Wireless MAC Filter:	Enable

*Wireless Network Mode:* Displays the wireless network mode of the access point: **11B Only**, **11G Only**, **11B/G Mixed**, or **11A**.

*Channel number:* Displays the RF channel: **auto** or a value from **1** (2.412 GHz) to **11** (2.462 GHz).

*Network name (SSID):* Displays the network name, also referred to as the SSID (service set identifier), of the access point.

*Data rate:* Displays the rate of data transmission: **auto** or a value from **1 Mbps** to **54 Mbps**.

*Security mode:* Displays the security mode of the access point: **Static WEP, Enterprise WEP, WPA-PSK with TKIP, WPA-PSK with AES, WPA2-PSK with TKIP, WPA2-PSK with AES, Enterprise WPA with AES, Enterprise WPA with TKIP, Enterprise WPA2 with AES, or Enterprise WPA2 with TKIP.** If security mode is disabled, the setting is displayed as **Open System**.

*SSID broadcasts:* Displays whether SSID broadcasting is enabled or disabled.

*Wireless MAC Filter:* Displays whether MAC address filtering is enabled or disabled.

**DHCP Server Settings:** The *DHCP Server Settings* section of the “Bridge/AP Settings and Info” page displays whether DHCP functionality is disabled or enabled. The following shows the *DHCP Server Settings* section of the page when DHCP functionality is enabled.

**“Bridge/AP Settings and Info” Page – DHCP Server Settings**

DHCP Server Settings	
Default gateway:	192.168.100.1
Subnet mask:	255.255.255.0
Primary DNS server:	192.168.100.1
Secondary DNS server:	192.168.100.10
First allocatable IP address:	192.168.100.100
Allocatable IP address count:	100

*Default gateway:* Displays the IP address of the access point, which functions as the default gateway.

*Subnet mask:* Displays the subnet mask of the network.

*Primary DNS server:* Displays the IP address of the primary DNS server.

*Secondary DNS server:* Displays the IP address of the secondary DNS server.

*First allocatable IP address:* Displays the first IP address to be assigned to a client device by the access point.

*Allocatable IP address count:* Displays the maximum number of devices to which the access point can assign IP addresses, that is, the maximum number of DHCP users.

**Static DHCP Mappings:** The *Static DHCP Mappings* section of the “Bridge/AP Settings and Info” page displays the static DHCP mapping(s) that are enabled.

**Advanced Settings:** The following shows the *Advanced Settings* section of the “Bridge/AP Settings and Info” page.

**“Bridge/AP Settings and Info” Page – Advanced Settings**

Advanced Settings	
SNMP:	Enable
UPNP:	Enable

*SNMP:* Displays whether SNMP is enabled or disabled.

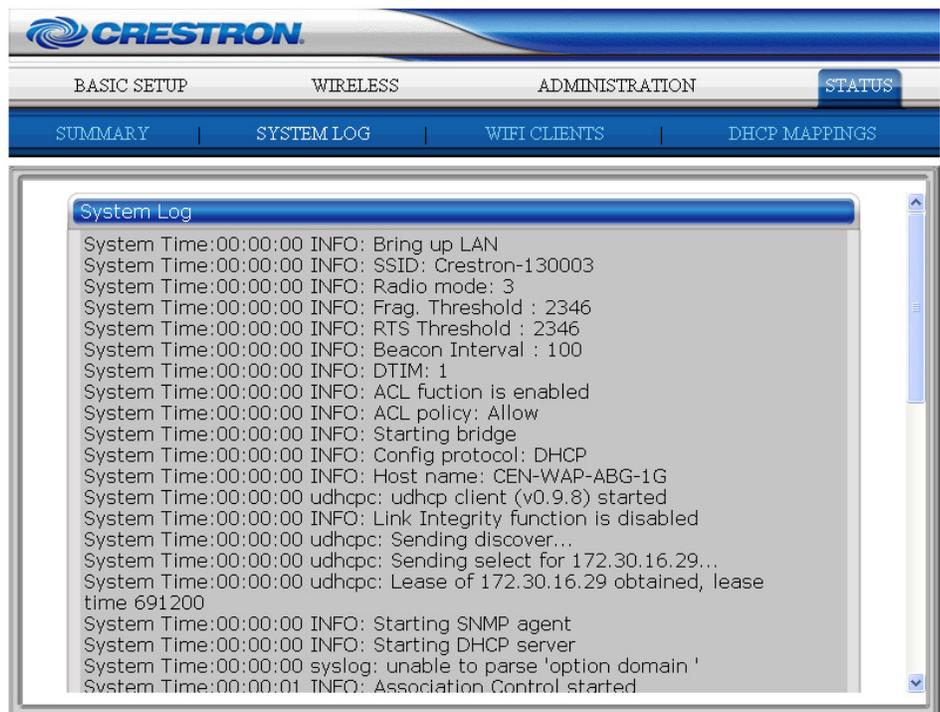
*UPNP:* Displays whether UPnP is enabled or disabled.

**Viewing the System Log**

For troubleshooting purposes, you can view a log of system events that include the following:

- General system events, which consist of system and network connectivity status changes.
- Built-in access point system events, which consist of wireless client association and authentication status changes.
- MIB II traps, which display Cold Start, Warm Start, Link Up, Link Down, and SNMP Authentication Failure trap messages.
- RADIUS user authentication system events, which display RADIUS user authentication status changes.

To view a log of system events, click the *STATUS* tab and then click the *SYSTEM LOG* subtab. The “System Log” page opens.

**“System Log” Page Example**

**NOTE:** To refresh the screen, click **Refresh** at the bottom of the screen.

*Viewing the Status of  
Associated Wireless Clients*

To view the status of wireless clients that are associated with the access point, click the *STATUS* tab and then click the *WIFI CLIENTS* subtab. The “Associated Wireless Clients” page opens.

*“Associated Wireless Clients” Page*

Wireless Clients Status						
No.	MAC Address	Tx Bytes	Rx Bytes	Data Rate	Signal Strength	Last Activity Time (secs)
1	00:0b:6c:37:42:e7	17773893	37081526	11 Mbps	53	0.710
2	00:16:6f:b1:c6:81	6964807	12732388	48 Mbps	39	2.980

Refresh

**NOTE:** To refresh the screen, click **Refresh** at the bottom of the screen.

For each associated client, the Wireless Clients Status table displays the following information:

*No.:* Displays the numerical order in which the client was associated with the access point.

*MAC Address:* Displays the MAC address of the client.

*Tx Bytes:* Displays the number of bytes transmitted by the access point to the client since its association with the access point.

*Rx Bytes:* Displays the number of bytes received by the access point from the client since its association with the access point.

*Data Rate:* Displays the connection speed between the client and the access point in megabits per second (Mbps).

**NOTE:** Because some clients measure the speed of the network differently than the access point, the data rate shown may not match the data rate reported by your wireless clients.

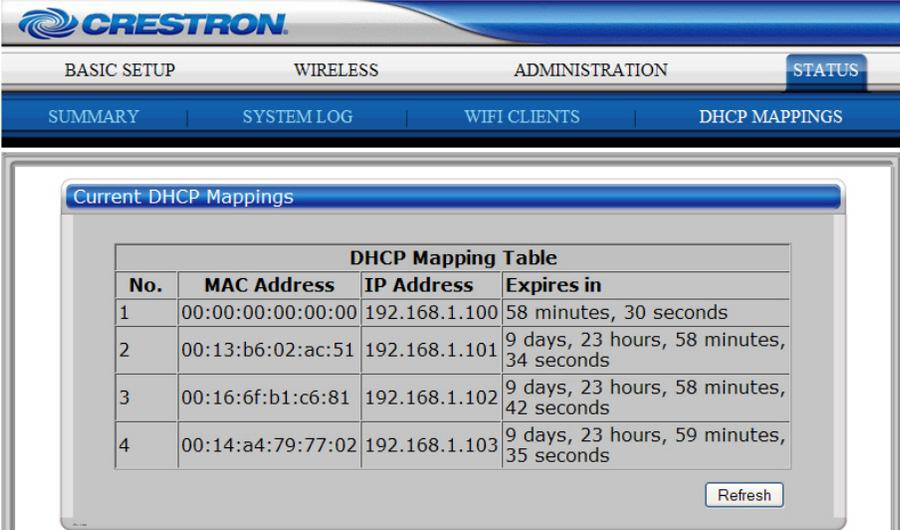
*Signal Strength:* Displays the strength of the radio signal in dBm, which measures the quality of the client’s wireless connection. A value above 45 is very good. A value of 30 is acceptable. A value below 30 may indicate connection issues. The value changes as the distance between the client and the access point changes.

*Last Activity Time (secs):* Displays the time in seconds that wireless data was last transmitted to or received from the client.

**Viewing DHCP Mappings**

You can view the status of current static and dynamic DHCP mappings. Static DHCP mappings are set in the *Static DHCP Mappings* section of the “DHCP Server” configuration page. Dynamic DHCP mappings are based on the *Starting IP address* and *Maximum number of DHCP users* settings of the “DHCP Server” page. For additional information about DHCP server configuration, refer to “Configuring DHCP Server Settings” on page 23.

To view the status of current DHCP mappings, click the *STATUS* tab and then click the *DHCP MAPPINGS* subtab. The “Current DHCP Mappings” page opens.

**“Current DHCP Mappings” Page**


The screenshot shows the Crestron web interface with the following navigation tabs: BASIC SETUP, WIRELESS, ADMINISTRATION, and STATUS. Under the STATUS tab, there are subtabs: SUMMARY, SYSTEM LOG, WIFI CLIENTS, and DHCP MAPPINGS. The DHCP MAPPINGS subtab is selected, displaying the 'Current DHCP Mappings' page. The page contains a table titled 'DHCP Mapping Table' with the following data:

No.	MAC Address	IP Address	Expires in
1	00:00:00:00:00:00	192.168.1.100	58 minutes, 30 seconds
2	00:13:b6:02:ac:51	192.168.1.101	9 days, 23 hours, 58 minutes, 34 seconds
3	00:16:6f:b1:c6:81	192.168.1.102	9 days, 23 hours, 58 minutes, 42 seconds
4	00:14:a4:79:77:02	192.168.1.103	9 days, 23 hours, 59 minutes, 35 seconds

A 'Refresh' button is located at the bottom right of the table.

**NOTE:** To refresh the screen, click **Refresh** at the bottom of the screen.

For each DHCP mapping, the DHCP Mapping Table displays the following information:

*No.:* Displays the numerical order in which a wireless client was assigned a static DHCP mapping.

*MAC Address:* Displays the MAC address of the client.

*Expires in:* Displays the expiration time of the DHCP mapping.

## Problem Solving

### Troubleshooting

The following table provides corrective action for possible trouble situations. If further assistance is required, please contact a Crestron customer service representative.

#### *CEN-WAP-ABG Troubleshooting*

TROUBLE	POSSIBLE CAUSE(S)	CORRECTIVE ACTION
<b>LAN</b> LED does not illuminate.	Network cable is not connected to the <b>NETWORK PoE</b> port on the rear of the access point or to the 10BaseT/100BaseTX compatible device.	Verify network cable connection to the <b>NETWORK PoE</b> port and to the network device.  Note that if a PWE-4803RU PoE injector is used and connects only to the access point, the <b>LAN</b> LED on the access point does not illuminate because no LAN data is present.
	Network cable is not the proper type.	Verify that network cable complies with EIA/TIA 568 and the CAT5 specification.
	Network cable is not the proper length.	Verify that network cable is the proper length. Cable length must not exceed 328 feet (100 meters).
	Fault exists with the network cable.	Replace the cable.
	10BaseT/100BaseTX compatible device is not powered on.	Power on the network device.
	Port is not functioning.	Replace the access point.
<b>LAN</b> LED illuminates but <b>Wi-Fi</b> LED does not illuminate.	RF signaling is not functioning.	Replace the access point.

*(Continued on following page)*

*CEN-WAP-ABG Troubleshooting (Continued)*

<b>TROUBLE</b>	<b>POSSIBLE CAUSE(S)</b>	<b>CORRECTIVE ACTION</b>
(CEN-WAP-ABG-1G only) Green LED on front Ethernet port does not illuminate.	Network cable is not connected to the front Ethernet port or to the 10BaseT/100BaseTX compatible device.	Verify network cable connection to the front Ethernet port and to the network device.
	Network cable is not the proper type.	Verify that network cable complies with EIA/TIA 568 and the CAT5 specification.
	Network cable is not the proper length.	Verify that network cable is the proper length. Cable length must not exceed 328 feet (100 meters).
	Fault exists with the network cable.	Replace the cable.
	10BaseT/100BaseTX compatible device is not powered on.	Power on the network device.
	Port is not functioning.	Replace the access point.
Low signal strength	Equipment is operating on the same frequency level as 802.11b/g, or interference exists from cordless phones, microwaves, and other electrical equipment.	Perform a site survey and correct wireless network interference issues as appropriate. For detailed information, refer to the latest version of the Best Practices for Installation and Setup of Crestron RF Products Reference Guide (Doc. 6689), which is available from the Crestron website.
	No antenna or improper antenna is connected.	Connect the proper antenna (included with the access point).

*(Continued on following page)*

*CEN-WAP-ABG Troubleshooting (Continued)*

TROUBLE	POSSIBLE CAUSE(S)	CORRECTIVE ACTION
Wireless network device cannot connect to the access point and cannot see the SSID.	Errors exist with the configuration of the access point.	<p>Check that the operational mode is set to <b>WiFi Access Point</b>. For additional information, refer to “Configuring Operational Mode” on page 23.</p> <p>Check that the radio mode (802.11a/b/g) is compatible with the network device.</p> <p>Check that the SSID broadcast is enabled. For additional information, refer to “Configuring IEEE 802.11 Security Settings” on page 29.</p>
	Wireless device is not within range of the access point.	Check that the wireless device is within range of the access point.
Wireless network device cannot connect to the access point but can see the SSID.	Errors exist with the configuration of the access point.	<p>Check the security settings and network key.</p> <p>If MAC filtering is enabled, check that the wireless device is configured on the MAC filter list. For additional information, refer to “Configuring MAC Filters” on page 33.</p>

## Reference Documents

The latest version of all documents mentioned within the guide can be obtained from the Crestron website ([www.crestron.com/manuals](http://www.crestron.com/manuals)). This link will provide a list of product manuals arranged in alphabetical order by model number.

### *List of Related Reference Documents*

DOCUMENT TITLE
Best Practices for Installation and Setup of Crestron RF Products Reference Guide
CEN-WAP-ABG-1G Wireless Access Point Quickstart Guide
CEN-WAP-ABG-CM Wireless Access Point Quickstart Guide
Crestron e-Control Reference Guide

## Further Inquiries

If you cannot locate specific information or have questions after reviewing this guide, please take advantage of Crestron's award winning customer service team by calling Crestron at 1-888-CRESTRON [1-888-273-7876].

You can also log onto the online help section of the Crestron website ([www.crestron.com/onlinehelp](http://www.crestron.com/onlinehelp)) to ask questions about Crestron products. First-time users will need to establish a user account to fully benefit from all available features.

## Future Updates

As Crestron improves functions, adds new features and extends the capabilities of the CEN-WAP-ABG wireless access points, additional information may be made available as manual updates. These updates are solely electronic and serve as intermediary supplements prior to the release of a complete technical documentation revision.

Check the Crestron website periodically for manual update availability and its relevance. Updates are identified as an “Addendum” in the Download column.

---

## Software License Agreement

This License Agreement (“Agreement”) is a legal contract between you (either an individual or a single business entity) and Crestron Electronics, Inc. (“Crestron”) for software referenced in this guide, which includes computer software and as applicable, associated media, printed materials and “online” or electronic documentation (the “Software”).

BY INSTALLING, COPYING OR OTHERWISE USING THE SOFTWARE, YOU REPRESENT THAT YOU ARE AN AUTHORIZED DEALER OF CRESTRON PRODUCTS OR A CRESTRON AUTHORIZED INDEPENDENT PROGRAMMER AND YOU AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT INSTALL OR USE THE SOFTWARE.

IF YOU HAVE PAID A FEE FOR THIS LICENSE AND DO NOT ACCEPT THE TERMS OF THIS AGREEMENT, CRESTRON WILL REFUND THE FEE TO YOU PROVIDED YOU (1) CLICK THE DO NOT ACCEPT BUTTON, (2) DO NOT INSTALL THE SOFTWARE AND (3) RETURN ALL SOFTWARE, MEDIA AND OTHER DOCUMENTATION AND MATERIALS PROVIDED WITH THE SOFTWARE TO CRESTRON AT: CRESTRON ELECTRONICS, INC., 15 VOLVO DRIVE, ROCKLEIGH, NEW JERSEY 07647, WITHIN 30 DAYS OF PAYMENT.

### LICENSE TERMS

Crestron hereby grants You and You accept a nonexclusive, nontransferable license to use the Software (a) in machine readable object code together with the related explanatory written materials provided by Crestron (b) on a central processing unit (“CPU”) owned or leased or otherwise controlled exclusively by You and (c) only as authorized in this Agreement and the related explanatory files and written materials provided by Crestron.

If this software requires payment for a license, you may make one backup copy of the Software, provided Your backup copy is not installed or used on any CPU. You may not transfer the rights of this Agreement to a backup copy unless the installed copy of the Software is destroyed or otherwise inoperable and You transfer all rights in the Software.

You may not transfer the license granted pursuant to this Agreement or assign this Agreement without the express written consent of Crestron.

If this software requires payment for a license, the total number of CPUs on which all versions of the Software are installed may not exceed one per license fee (1) and no concurrent, server or network use of the Software (including any permitted back-up copies) is permitted, including but not limited to using the Software (a) either directly or through commands, data or instructions from or to another computer (b) for local, campus or wide area network, internet or web hosting services or (c) pursuant to any rental, sharing or “service bureau” arrangement.

The Software is designed as a software development and customization tool. As such Crestron cannot and does not guarantee any results of use of the Software or that the Software will operate error free and You acknowledge that any development that You perform using the Software or Host Application is done entirely at Your own risk.

The Software is licensed and not sold. Crestron retains ownership of the Software and all copies of the Software and reserves all rights not expressly granted in writing.

### OTHER LIMITATIONS

You must be an Authorized Dealer of Crestron products or a Crestron Authorized Independent Programmer to install or use the Software. If Your status as a Crestron Authorized Dealer or Crestron Authorized Independent Programmer is terminated, Your license is also terminated.

You may not rent, lease, lend, sublicense, distribute or otherwise transfer or assign any interest in or to the Software.

You may not reverse engineer, decompile or disassemble the Software.

You agree that the Software will not be shipped, transferred or exported into any country or used in any manner prohibited by the United States Export Administration Act or any other export laws, restrictions or regulations (“Export Laws”). By downloading or installing the Software You (a) are certifying that You are not a national of Cuba, Iran, Iraq, Libya, North Korea, Sudan, Syria or any country to which the United States embargoes goods (b) are certifying that You are not otherwise prohibited from receiving the Software and (c) You agree to comply with the Export Laws.

If any part of this Agreement is found void and unenforceable, it will not affect the validity of the balance of the Agreement, which shall remain valid and enforceable according to its terms. This Agreement may only be modified by a writing signed by an authorized officer of Crestron. Updates may be licensed to You by Crestron with additional or different terms. This is the entire agreement between Crestron and You relating to the Software and it supersedes any prior representations, discussions, undertakings, communications or advertising relating to the Software. The failure of either party to enforce any right or take any action in the event of a breach hereunder shall constitute a waiver unless expressly acknowledged and set forth in writing by the party alleged to have provided such waiver.

If You are a business or organization, You agree that upon request from Crestron or its authorized agent, You will within thirty (30) days fully document and certify that use of any and all Software at the time of the request is in conformity with Your valid licenses from Crestron or its authorized agent.

Without prejudice to any other rights, Crestron may terminate this Agreement immediately upon notice if you fail to comply with the terms and conditions of this Agreement. In such event, you must destroy all copies of the Software and all of its component parts.

#### PROPRIETARY RIGHTS

**Copyright.** All title and copyrights in and to the Software (including, without limitation, any images, photographs, animations, video, audio, music, text and “applets” incorporated into the Software), the accompanying media and printed materials and any copies of the Software are owned by Crestron or its suppliers. The Software is protected by copyright laws and international treaty provisions. Therefore, you must treat the Software like any other copyrighted material, subject to the provisions of this Agreement.

**Submissions.** Should you decide to transmit to Crestron’s website by any means or by any media any materials or other information (including, without limitation, ideas, concepts or techniques for new or improved services and products), whether as information, feedback, data, questions, comments, suggestions or the like, you agree such submissions are unrestricted and shall be deemed non-confidential and you automatically grant Crestron and its assigns a non-exclusive, royalty-free, worldwide, perpetual, irrevocable license, with the right to sublicense, to use, copy, transmit, distribute, create derivative works of, display and perform the same.

**Trademarks.** CRESTRON and the Swirl Logo are registered trademarks of Crestron Electronics, Inc. You shall not remove or conceal any trademark or proprietary notice of Crestron from the Software including any back-up copy.

#### GOVERNING LAW

This Agreement shall be governed by the laws of the State of New Jersey, without regard to conflicts of laws principles. Any disputes between the parties to the Agreement shall be brought in the state courts in Bergen County, New Jersey or the federal courts located in the District of New Jersey. The United Nations Convention on Contracts for the International Sale of Goods shall not apply to this Agreement.

#### CRESTRON LIMITED WARRANTY

CRESTRON warrants that: (a) the Software will perform substantially in accordance with the published specifications for a period of ninety (90) days from the date of receipt and (b) that any hardware accompanying the Software will be subject to its own limited warranty as stated in its accompanying written material. Crestron shall, at its option, repair or replace or refund the license fee for any Software found defective by Crestron if notified by you within the warranty period. The foregoing remedy shall be your exclusive remedy for any claim or loss arising from the Software.

CRESTRON shall not be liable to honor warranty terms if the product has been used in any application other than that for which it was intended or if it as been subjected to misuse, accidental damage, modification or improper installation procedures. Furthermore, this warranty does not cover any product that has had the serial number or license code altered, defaced, improperly obtained or removed.

Notwithstanding any agreement to maintain or correct errors or defects, Crestron shall have no obligation to service or correct any error or defect that is not reproducible by Crestron or is deemed in Crestron’s reasonable discretion to have resulted from (1) accident; unusual stress; neglect; misuse; failure of electric power, operation of the Software with other media not meeting or not maintained in accordance with the manufacturer’s specifications or causes other than ordinary use; (2) improper installation by anyone other than Crestron or its authorized agents of the Software that deviates from any operating procedures established by Crestron in the material and files provided to You by Crestron or its authorized agent; (3) use of the Software on unauthorized hardware or (4) modification of, alteration of or additions to the Software undertaken by persons other than Crestron or Crestron’s authorized agents.

ANY LIABILITY OF CRESTRON FOR A DEFECTIVE COPY OF THE SOFTWARE WILL BE LIMITED EXCLUSIVELY TO REPAIR OR REPLACEMENT OF YOUR COPY OF THE SOFTWARE WITH ANOTHER COPY OR REFUND OF THE INITIAL LICENSE FEE CRESTRON RECEIVED FROM YOU FOR THE DEFECTIVE COPY OF THE PRODUCT. THIS WARRANTY SHALL BE THE SOLE AND EXCLUSIVE REMEDY TO YOU. IN NO EVENT SHALL CRESTRON BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, SPECIAL OR PUNITIVE DAMAGES OF ANY KIND (PROPERTY OR ECONOMIC DAMAGES INCLUSIVE), EVEN IF A CRESTRON REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR OF ANY CLAIM BY ANY THIRD PARTY. CRESTRON MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO TITLE OR INFRINGEMENT OF THIRD-PARTY RIGHTS, MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY OTHER WARRANTIES, NOR AUTHORIZES ANY OTHER PARTY TO OFFER ANY WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY FOR THIS PRODUCT. THIS WARRANTY STATEMENT SUPERSEDES ALL PREVIOUS WARRANTIES.

---

## Return and Warranty Policies

### Merchandise Returns / Repair Service

1. No merchandise may be returned for credit, exchange or service without prior authorization from CRESTRON. To obtain warranty service for CRESTRON products, contact an authorized CRESTRON dealer. Only authorized CRESTRON dealers may contact the factory and request an RMA (Return Merchandise Authorization) number. Enclose a note specifying the nature of the problem, name and phone number of contact person, RMA number and return address.
2. Products may be returned for credit, exchange or service with a CRESTRON Return Merchandise Authorization (RMA) number. Authorized returns must be shipped freight prepaid to CRESTRON, 6 Volvo Drive, Rockleigh, N.J. or its authorized subsidiaries, with RMA number clearly marked on the outside of all cartons. Shipments arriving freight collect or without an RMA number shall be subject to refusal. CRESTRON reserves the right in its sole and absolute discretion to charge a 15% restocking fee plus shipping costs on any products returned with an RMA.
3. Return freight charges following repair of items under warranty shall be paid by CRESTRON, shipping by standard ground carrier. In the event repairs are found to be non-warranty, return freight costs shall be paid by the purchaser.

### CRESTRON Limited Warranty

CRESTRON ELECTRONICS, Inc. warrants its products to be free from manufacturing defects in materials and workmanship under normal use for a period of three (3) years from the date of purchase from CRESTRON, with the following exceptions: disk drives and any other moving or rotating mechanical parts, pan/tilt heads and power supplies are covered for a period of one (1) year; touchscreen display and overlay components are covered for 90 days; batteries and incandescent lamps are not covered.

This warranty extends to products purchased directly from CRESTRON or an authorized CRESTRON dealer. Purchasers should inquire of the dealer regarding the nature and extent of the dealer's warranty, if any.

CRESTRON shall not be liable to honor the terms of this warranty if the product has been used in any application other than that for which it was intended or if it has been subjected to misuse, accidental damage, modification or improper installation procedures. Furthermore, this warranty does not cover any product that has had the serial number altered, defaced or removed.

This warranty shall be the sole and exclusive remedy to the original purchaser. In no event shall CRESTRON be liable for incidental or consequential damages of any kind (property or economic damages inclusive) arising from the sale or use of this equipment. CRESTRON is not liable for any claim made by a third party or made by the purchaser for a third party.

CRESTRON shall, at its option, repair or replace any product found defective, without charge for parts or labor. Repaired or replaced equipment and parts supplied under this warranty shall be covered only by the unexpired portion of the warranty.

Except as expressly set forth in this warranty, CRESTRON makes no other warranties, expressed or implied, nor authorizes any other party to offer any warranty, including any implied warranties of merchantability or fitness for a particular purpose. Any implied warranties that may be imposed by law are limited to the terms of this limited warranty. This warranty statement supersedes all previous warranties.

#### Trademark Information

*All brand names, product names and trademarks are the sole property of their respective owners. Windows is a registered trademark of Microsoft Corporation. Windows95/98/Me/XP/Vista and WindowsNT/2000 are trademarks of Microsoft Corporation.*

This page is intentionally left blank.



Crestron Electronics, Inc.  
15 Volvo Drive Rockleigh, NJ 07647  
Tel: 888.CRESTRON  
Fax: 201.767.7576  
[www.crestron.com](http://www.crestron.com)

Operations & Installation Guide – DOC. 6695C  
(2022090)

04.09

Specifications subject to  
change without notice.