CEN-GW1 and CENI-GW1

Universal Wireless Gateway, ER Wireless, SG Wireless, and infiNET EX® Wireless Gateway

Product Manual

Crestron Electronics, Inc.

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

Regulatory Model: M201913001

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

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

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

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

Crestron, the Crestron logo, Crestron Toolbox, and infiNET EX are either trademarks or registered trademarks of Crestron Electronics, Inc. in the United States and/or other countries. Active Directory is either a trademark or registered trademark of Microsoft Corporation in the United States and/or other countries. Other trademarks, registered trademarks, and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Crestron disclaims any proprietary interest in the marks and names of others. Crestron is not responsible for errors in typography or photography.

©2021 Crestron Electronics, Inc.

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

NOTE: THE GRANTEE IS NOT RESPONSIBLE FOR ANY CHANGES OR MODIFICATIONS NOT EXPRESSLY APPROVED BY THE PARTY RESPONSIBLE FOR COMPLIANCE. SUCH MODIFICATIONS COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

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

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Contents

Web Configuration

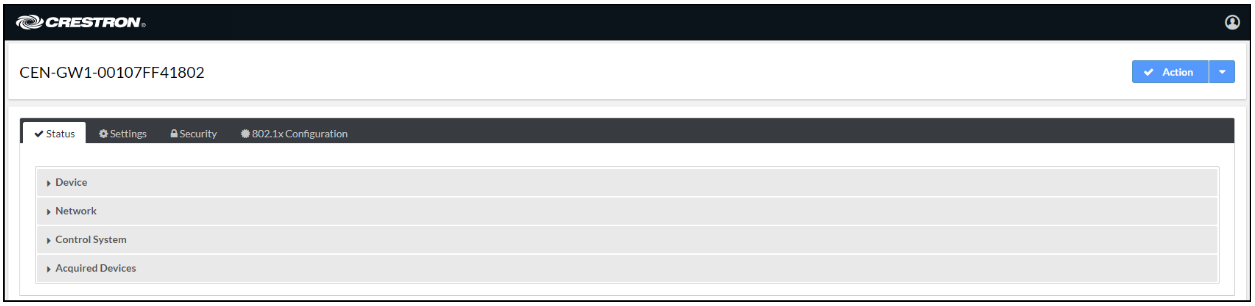
Monitor and configure the CEN-GW1 and CENI-GW1 using the built-in web configuration interface.

To access the web configuration:

1. Use the Device Discovery tool in Crestron Toolbox™ software to discover the device and its IP address on the network.
2. In a web browser, go to the IP address of the device.

> NOTE: If authentication is enabled for the gateway, an administrator username and password must be entered prior to accessing the web configuration interface. For more information on configuring authentication settings, refer to Authentication.

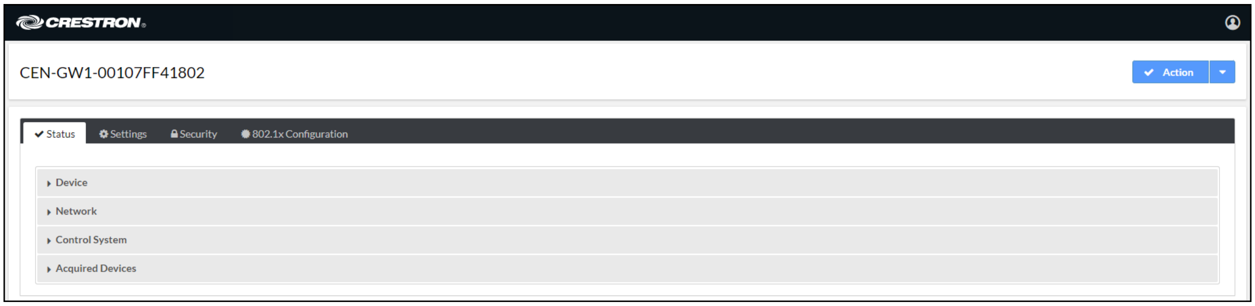
The web configuration provides tabs to view and configure device settings.



These tabs are provided:

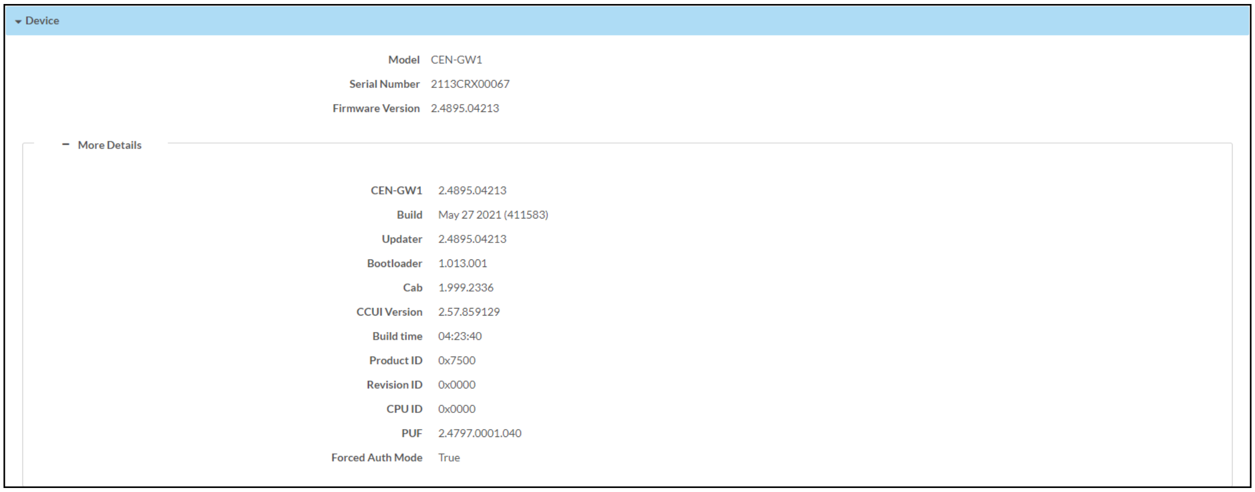
Status

Use the **Status** tab to view the device information.



Device

Use the **device** menu to view general device information such as the **Model**, **Serial Number**, and **Firmware Version**. Select More Details to view detailed device information such as the **Build**, **Bootloader**, **Build Time**, and more.

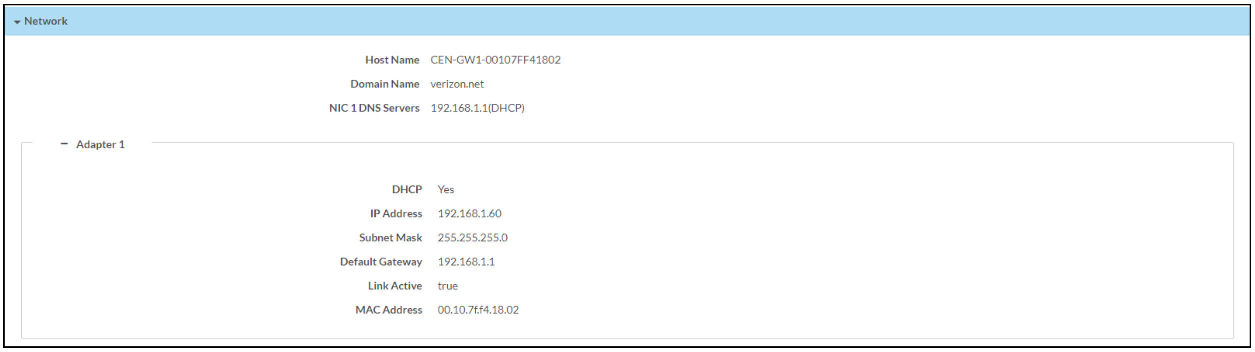


Model	CEN-GW1
Serial Number	2113CRX00067
Firmware Version	2.4895.04213

CEN-GW1	2.4895.04213
Build	May 27 2021 (411583)
Updater	2.4895.04213
Bootloader	1.013.001
Cab	1.999.2336
CCUI Version	2.57.859129
Build time	04:23:40
Product ID	0x7500
Revision ID	0x0000
CPU ID	0x0000
PUF	2.4797.0001.040
Forced Auth Mode	True

Network

Use the **Network** menu to view the **Host Name**, **Domain Name**, and **DNS Servers**. Select **Adapter 1** to view detailed network information such as **DHCP**, **IP Address**, and **Subnet Mask**.network settings of the device.



Network

Host Name CEN-GW1-00107FF41802

Domain Name verizon.net

NIC 1 DNS Servers 192.168.1.1(DHCP)

Adapter 1

DHCP Yes

IP Address 192.168.1.60

Subnet Mask 255.255.255.0

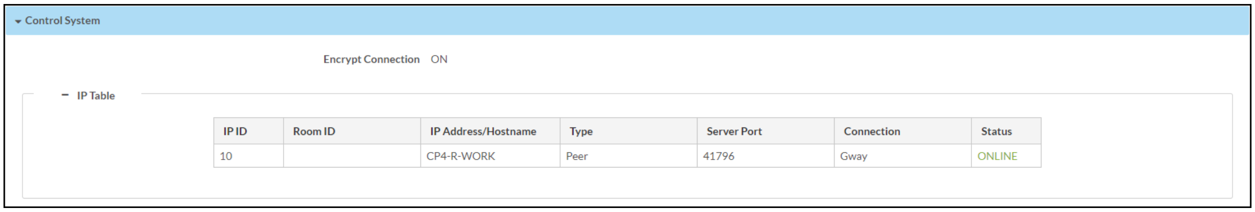
Default Gateway 192.168.1.1

Link Active true

MAC Address 00.10.7f.f4.18.02

Control System

Use the **Control System** menu to view the connection status to a control system.



Control System

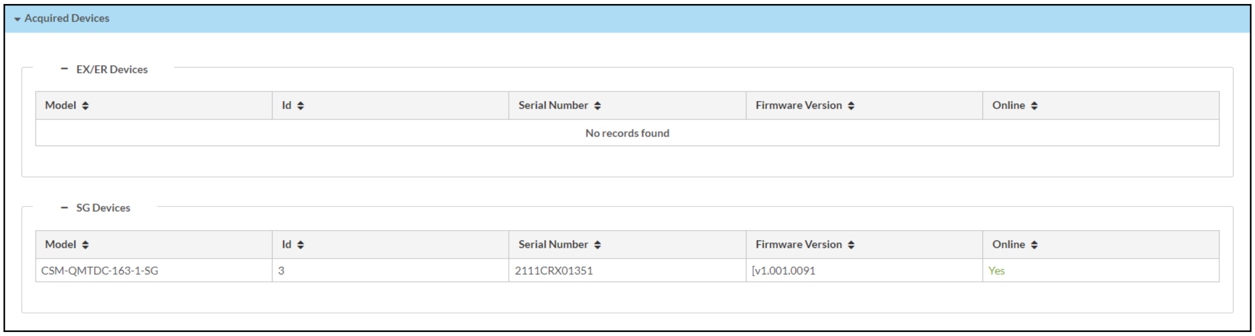
Encrypt Connection ON

IP Table

IP ID	Room ID	IP Address/Hostname	Type	Server Port	Connection	Status
10		CP4-R-WORK	Peer	41796	Gway	ONLINE

Acquired Devices

Use the **Acquired Devices** menu to view the SG, ER, and infiNET EX wireless devices that are acquired by the gateway.



Acquired Devices

EX/ER Devices

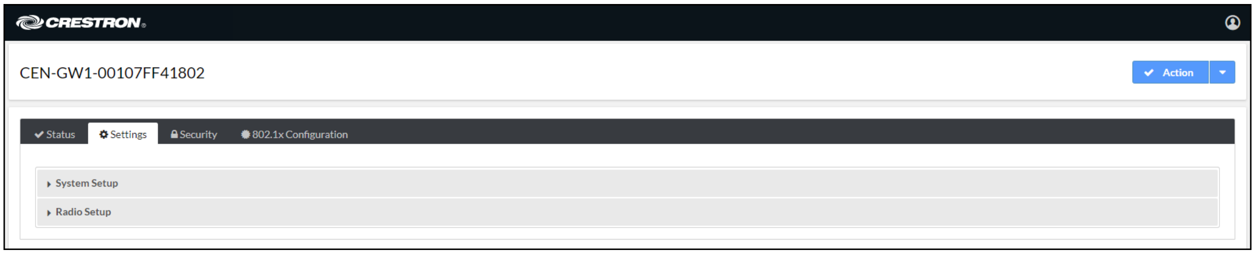
Model ⬍	Id ⬍	Serial Number ⬍	Firmware Version ⬍	Online ⬍
No records found				

SG Devices

Model ⬍	Id ⬍	Serial Number ⬍	Firmware Version ⬍	Online ⬍
CSM-QMTDC-163-1-SG	3	2111CRX01351	[v1.001.0091	Yes

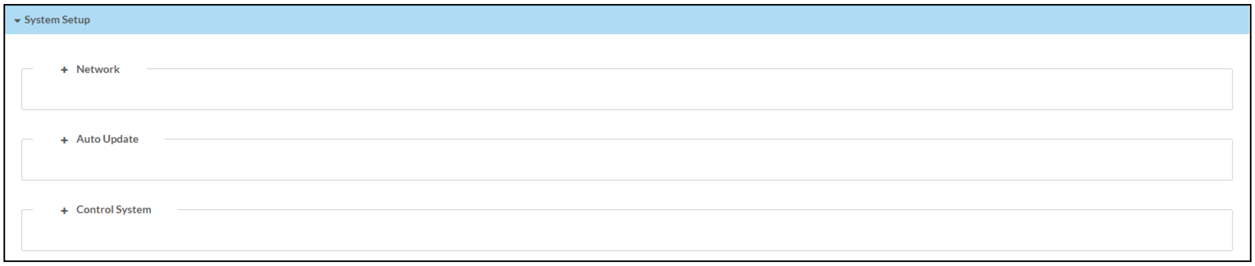
Settings

Delete this text and replace it with your own content.



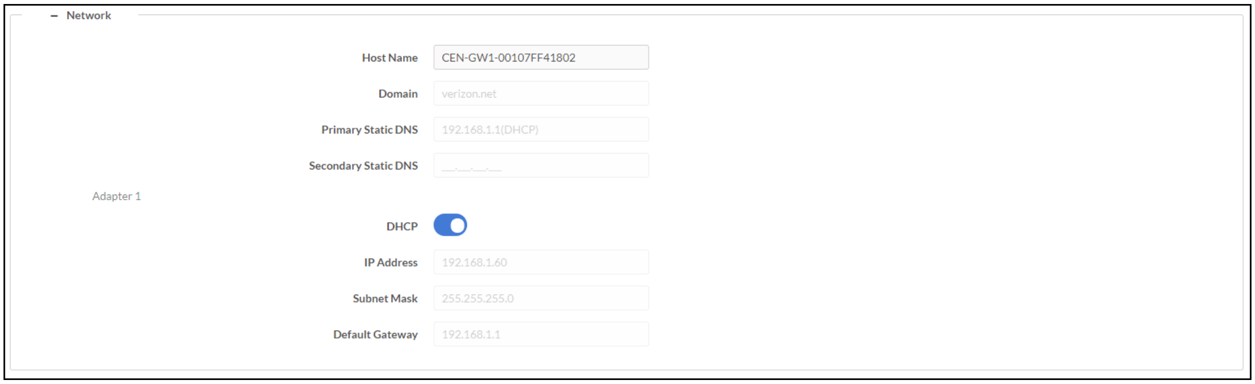
System Setup

Use the System Setup menu to configure the **Network**, **Auto Update**, and **Control System** settings.



Network

Use the **Network** menu to configure the connection to the Ethernet network. DHCP is turned on by default and the fields are automatically populated.



Host Name	CEN-GW1-00107FF41802
Domain	verizon.net
Primary Static DNS	192.168.1.1(DHCP)
Secondary Static DNS	___.___.___.___
DHCP	●
IP Address	192.168.1.60
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1

To set custom ethernet settings:

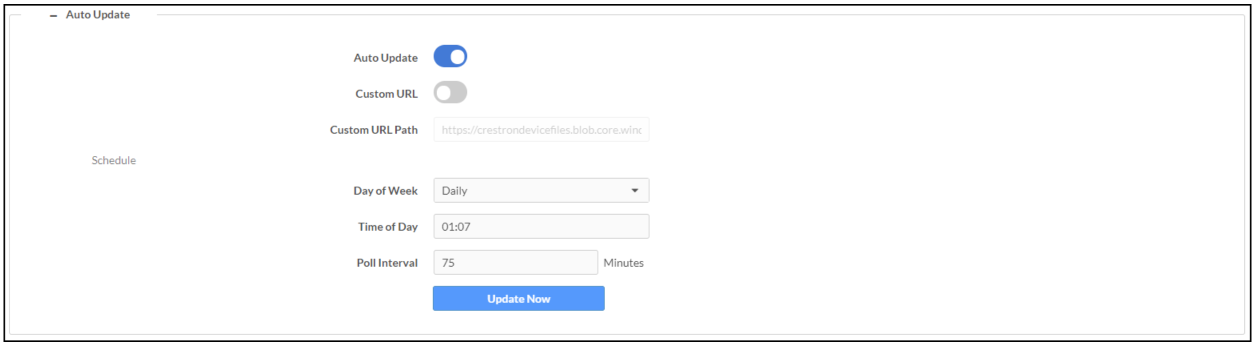
1. Deselect DHCP.
2. Enter the Domain, Primary Static DNS, and Secondary Static DNS information.

3. Enter the IP Address, Subnet Mask, and Default Gateway information.
4. In the **Actions** menu, select **Save Changes**.

Auto Update

Use the Auto Update menu to configure auto update settings. Auto Update is turned on by default and the fields are automatically populated.

Click **Auto Update** to configure time-based auto-update of firmware/apk or immediate update.



– Auto Update

Auto Update: On

Custom URL: Off

Custom URL Path: https://crestrondevicefiles.blob.core.winc

Schedule

Day of Week: Daily

Time of Day: 01:07

Poll Interval: 75 Minutes

To set the auto update time based on day of week and time:

1. Select a day from the Day of Week drop-down menu. To check for updates every day, select **Daily**.
2. Enter a time based on the 24-hour clock in the **Time of Day** box.
3. In the **Actions** menu, select **Save Changes**.

To set the auto update based on poll interval:

> NOTE: A non-zero value in the **Poll Interval (Minutes)** box overrides the **Day Of Week** and **Time Of Day** configuration.

1. Enter a time, in minutes, into the **Poll Interval** box. The range is 1 minute to 65535 minutes.
2. In the **Actions** menu, select **Save Changes**.

To use a custom auto update URL:

> NOTE: Do not change the default URL unless advised by a Crestron Tech Support Specialist.

1. Select **Custom URL**.
2. Enter a URL to a firmware server in the **Custom URL Path** box.

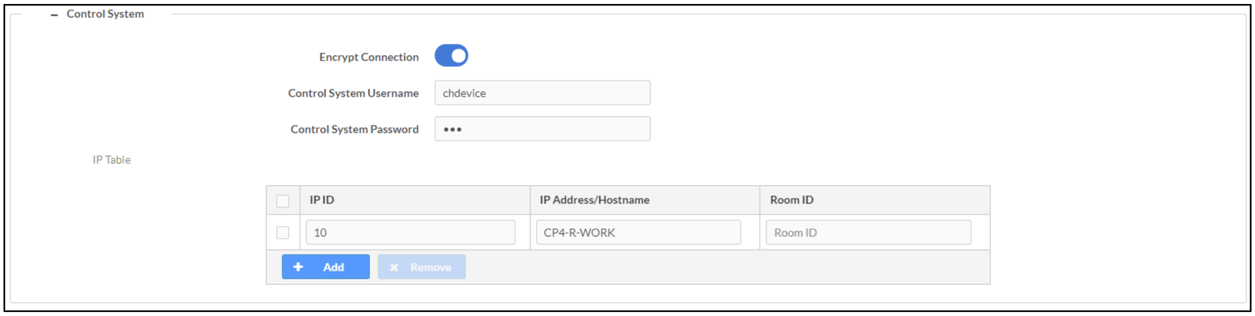
The device will connect to the firmware server provided in the **Custom URL Path** at the scheduled time.

Click **Check for Update** beside **Update Firmware Now** and/or **Update APK Now** to trigger the upgrade process immediately.

Control System

TBD

- Why Encrypt Connection?
- What is the username?
- what is the password?
- What is the IP Table



Encrypt Connection: ●

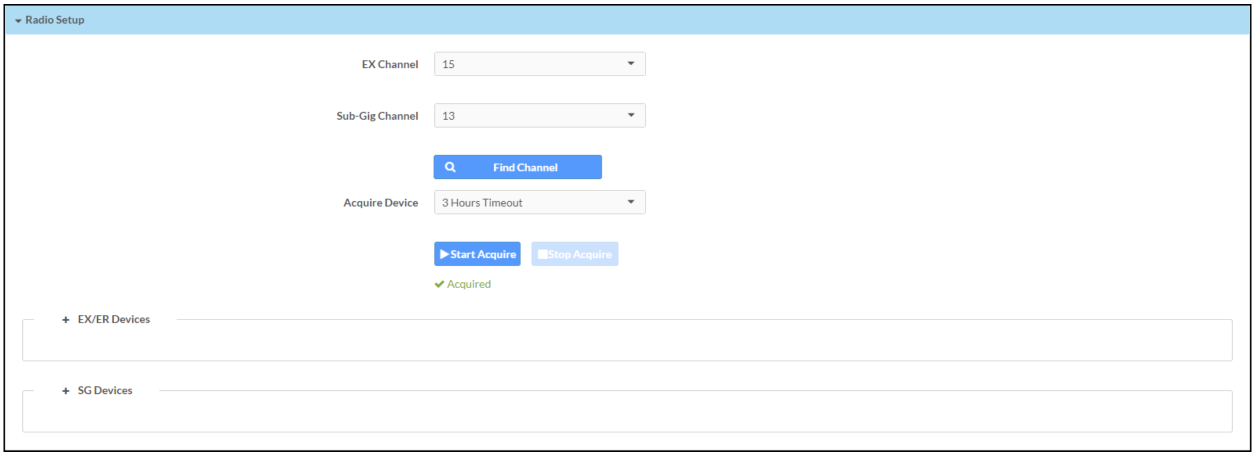
Control System Username: chdevice

Control System Password: •••

□	IP ID	IP Address/Hostname	Room ID
□	10	CP4-R-WORK	Room ID

Radio Setup

Use the Radio Setup menu to configure the SG, ER, and infiNET EX wireless radios and to acquire devices.



EX Channel: 15

Sub-Gig Channel: 13

Acquire Device: 3 Hours Timeout

✓ Acquired

Select RF Channel

Set the RF channels for the EX/ER radio and the SG radio:

NOTE: Scan the wireless network to determine the best RF channel for the EX/ER and SG radios. For details, refer to Settings (on page 4).

- Select an EX and ER channel from the **EX Channel** drop-down menu.
- Select an SG channel from the **SG Channel** drop-down menu.

Acquire Devices

To acquire devices to the gateway:

NOTES:

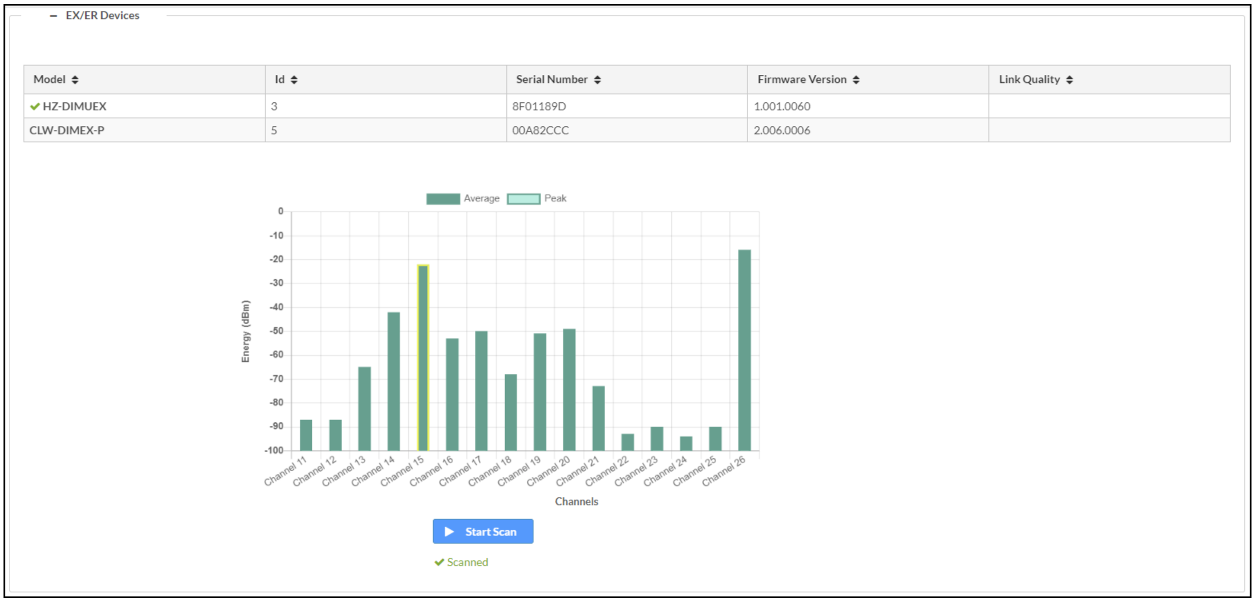
- Place the gateway into acquire mode prior to entering **Acquire** mode on a wireless device.
- Only one gateway can be in **Acquire** mode at a time.

1. Click **Start Acquire** to enter **Acquire** mode.
2. On an SG, ER, or infiNET EX wireless device, enter **Acquire** mode. For details, refer to the wireless device's instructions.
3. After all wireless devices are acquired, select **Stop Acquire** to exit **Acquire** mode.

Find Channels - What does Find Channels do?

EX/ER Devices

The devices that are acquired to the EX and ER radio are displayed along with the energy scan chart.



− EX/ER Devices

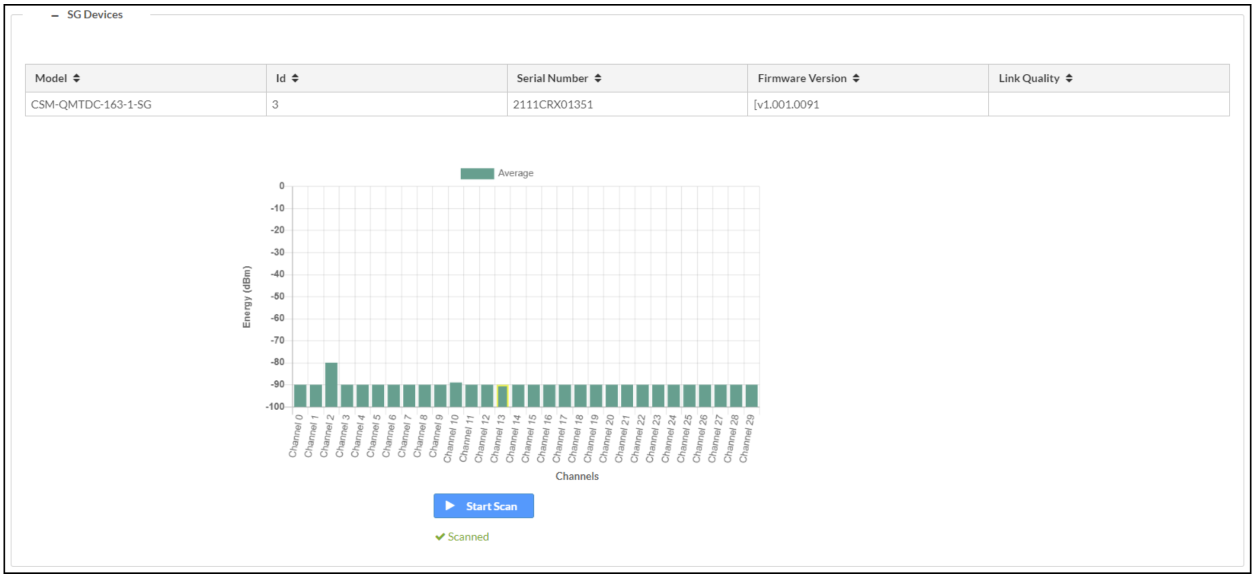
Model ⬍	Id ⬍	Serial Number ⬍	Firmware Version ⬍	Link Quality ⬍
✓ HZ-DIMUEX	3	8F01189D	1.001.0060	
CLW-DIMEX-P	5	00A82CCC	2.006.0006	

To scan the wireless network:

1. In the EX/ER Devices, select **Start Scan**.
2. The wireless network is scanned and displays the **Energy (dBm)** for the **Channels**.

SG Devices

The devices that are acquired to the SG radio are displayed along with the energy scan chart.



– SG Devices

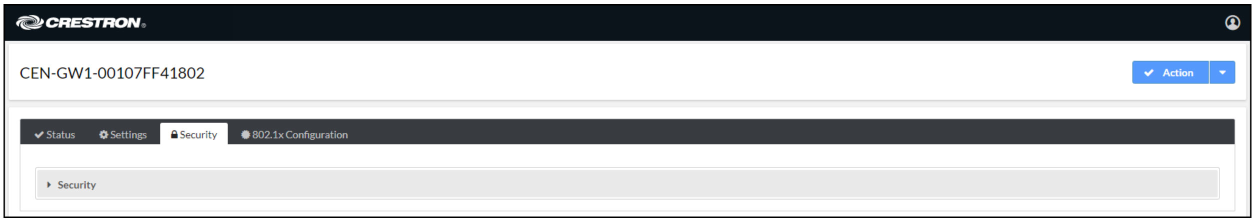
Model ⬍	Id ⬍	Serial Number ⬍	Firmware Version ⬍	Link Quality ⬍
CSM-QMTDC-163-1-SG	3	2111CRX01351	[v1.001.0091	

To scan the wireless network:

1. In the SG Devices menu, select **Start Scan**.
2. The wireless network is scanned and displays the **Energy (dBm)** for the **Channels**.

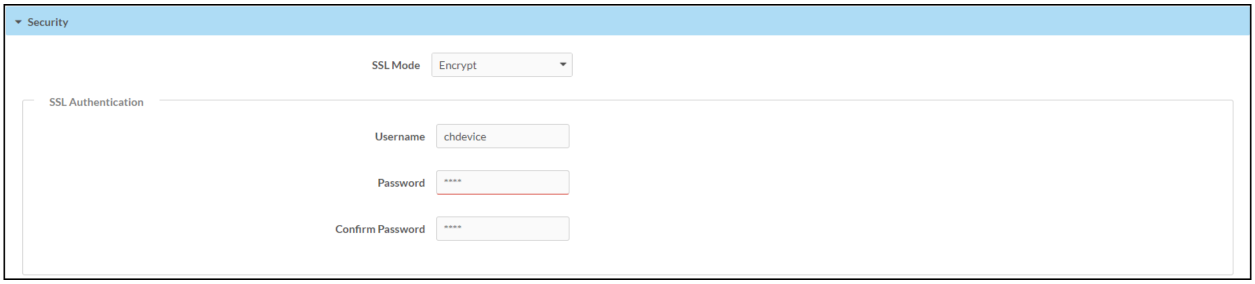
Security

Click the **Security** tab to configure security for users and groups and to allow different levels of access to the functions of the device.



SSL

Why change SSL mode? What does SSL Mode do?



SSL Mode: Encrypt

Username: chdevice

Password: ****

Confirm Password: ****

Select a mode from the **SSL Mode** drop-down menu.

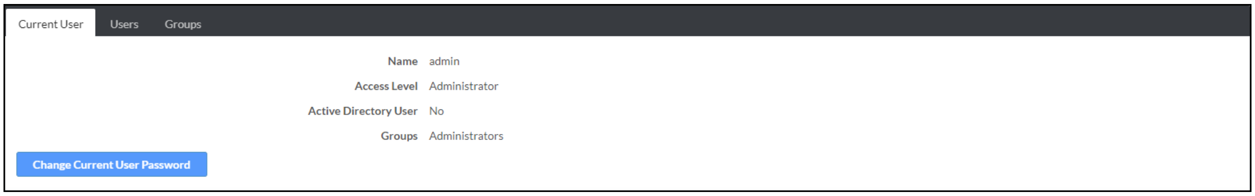
- **Encrypt and Validation:** The gateway will require a username and password to validate an encrypted SSL connection.
- **Encrypt:** The gateway will use an encrypted SSL connection
- **OFF:** The gateway will not use an SSL connection.

Is SSL Authentication only available for Encrypt and Validation??

To set the SSL Authentication, enter the **Username**, **Password**, and **Confirm Password**.

Current User

Use the **Current User** tab to view the current user's Name, Access Level, Active Directory User status, and Groups. The password for the current user can also be changed.



Name admin
Access Level Administrator
Active Directory User No
Groups Administrators

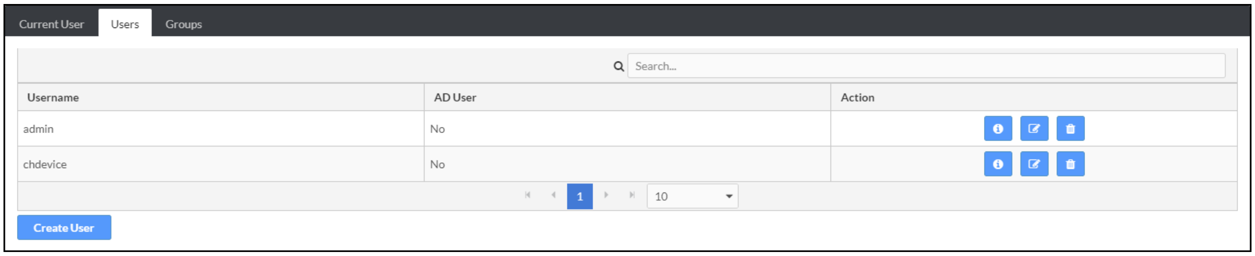
To change the current user's password:

1. Click **Change Current User Password**.
2. Enter the current user's password in the Current Password box.
3. Enter a new password in the Password and Confirm Password boxes.
4. Click **Yes**.

Users

Use the **Users** tab to manage authorized users. A list of authorized users is displayed.

Click ⓘ **Information** to view details about a user.



Username	AD User	Action
admin	No	ⓘ ✎ 🗑
chdevice	No	ⓘ ✎ 🗑

Edit a User

1. Click ✎ **Edit**.
2. If the user is a member of the Active Directory® credential management group, select **Active Directory User**.
3. Enter a password in the **Password** and **Confirm Password** boxes.
4. Select a group from the **Group** drop-down menu.
5. Click **Yes**.

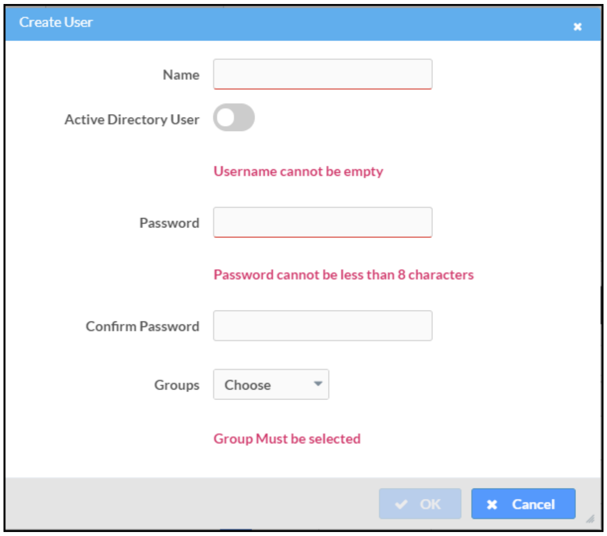
Delete a User

NOTE: The Admin user cannot be deleted.

1. Click 🗑 **Delete**.
2. In the confirmation dialog, click **Yes**.

Create a User

1. Click **Create User**.
2. Enter a **Username** in the **Name** box.
3. If the user is a member of the Active Directory® credential management group, select **Active Directory User**.



Create User ×

Name

Active Directory User

Username cannot be empty

Password

Password cannot be less than 8 characters

Confirm Password

Groups: Choose

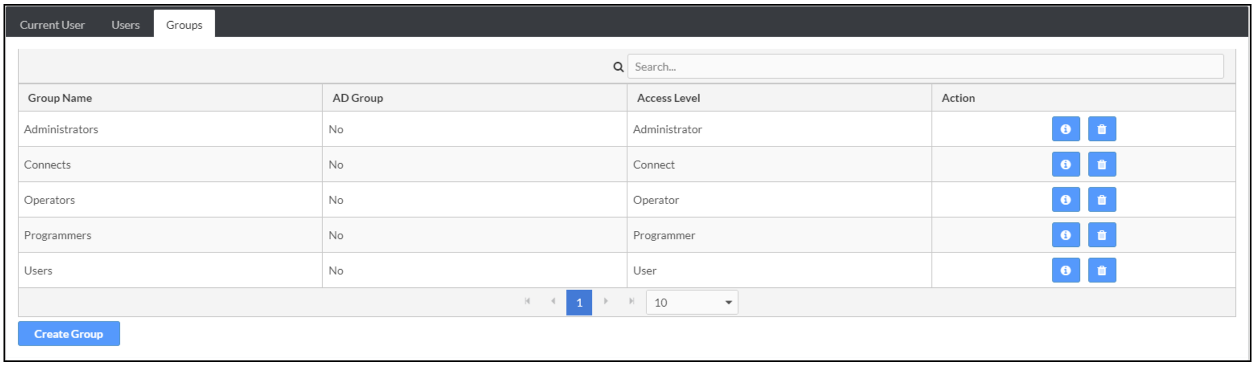
Group Must be selected

4. Click **Yes**.

Groups

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

Click ℹ **Information** to view details about a group.



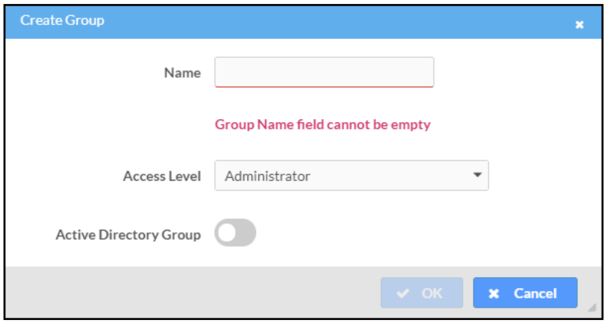
Group Name	AD Group	Access Level	Action
Administrators	No	Administrator	ℹ 🗑
Connects	No	Connect	ℹ 🗑
Operators	No	Operator	ℹ 🗑
Programmers	No	Programmer	ℹ 🗑
Users	No	User	ℹ 🗑

Delete a Group

1. Click 🗑 **Delete**.
2. In the confirmation dialog, click **Yes**.

Create a Group

1. Click **Create Group**.
2. Enter a **Group Name** in the **Name** box.
3. Select an access level from the **Access Level** drop-down menu.
4. If the user is a member of the Active Directory® credential management group, select **Active Directory User**.



Create Group

Name

Group Name field cannot be empty

Access Level: Administrator

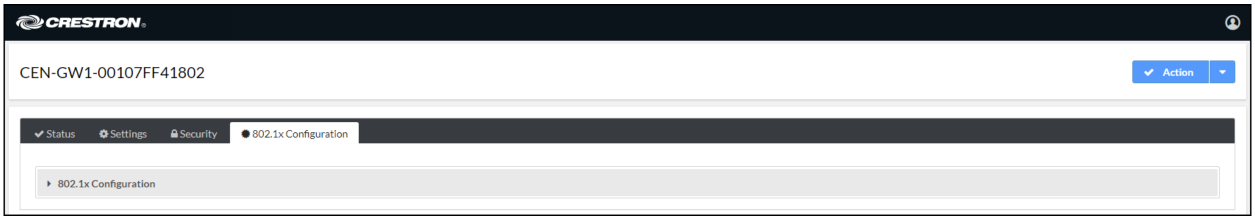
Active Directory Group

5. Click **Yes**.

802.1x Configuration

The 802.1X standard is an IEEE network standard designed to enhance the security of wireless and Ethernet LANs. The standard relies on the exchange of messages between the device and the network's host, or authentication server.

The device has built-in support for the 802.1X standard to allow communication with the authentication server and access to protected corporate networks.



Enable **IEEE 802.1x Configuration** and select the desired method of authentication.

Turn On IEEE 802.1x Authentication

To turn on authentication, select **IEEE 802.1x Authentication**.

Select an Authentication Method

To select an authentication method, select **EAP-TLS Certificate** or **EAP MSCHAP V2- password** from the **Authentication Method** drop-down menu.

If **EAP MSCHAP V2- password** is selected, enter the **Domain**, **Username**, and **Password**.

Server Validation

To turn on server validation:

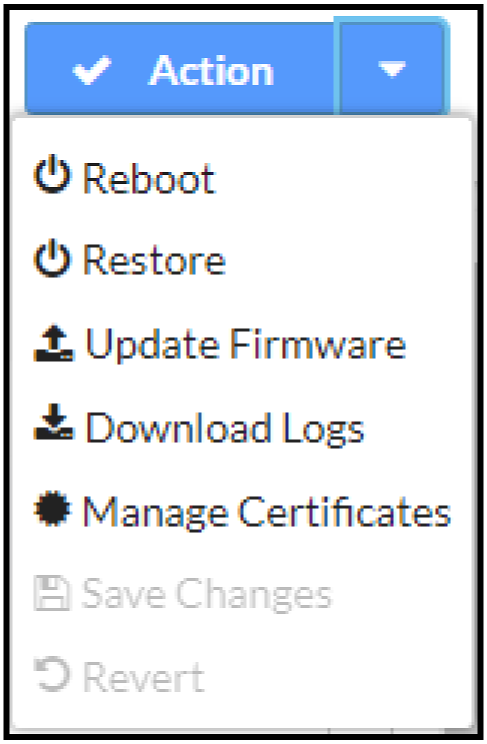
1. Select **Enable Authentication Server Validation**.
2. Select certificates from the **Selected Trusted Certificate Authorities** list.

> NOTE: To load a custom certificate, go to **Actions > Manage Certificates**. For details, refer to Manage Certificates (on page 15).

Action

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

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



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

If a reboot is required after changes have been saved, a dialog box is displayed asking whether the reboot should be performed. Select **OK** to reboot the device or **Cancel** to cancel the reboot.

The Action menu provides the following selections.

Reboot

To restart the gateway, select **Reboot** and then **Yes, Reboot Now**.

Restore

To restore the device settings to their factory default, select **Restore** and then **Yes** to confirm.

Update Firmware

To upgrade the device firmware:

NOTE: Do not turn off the device or stop the upgrade process until the device is upgraded. After the upgrade, the device will reboot.

NOTE: For time-based auto update of the firmware, refer to the Auto Update (on page 5).

1. Visit www.crestron.com/firmware and download the latest firmware.
2. Select **Upload Firmware** and then select **Browse**.
3. Select the firmware file and then select Open.
4. To upload the firmware, select **Load**.

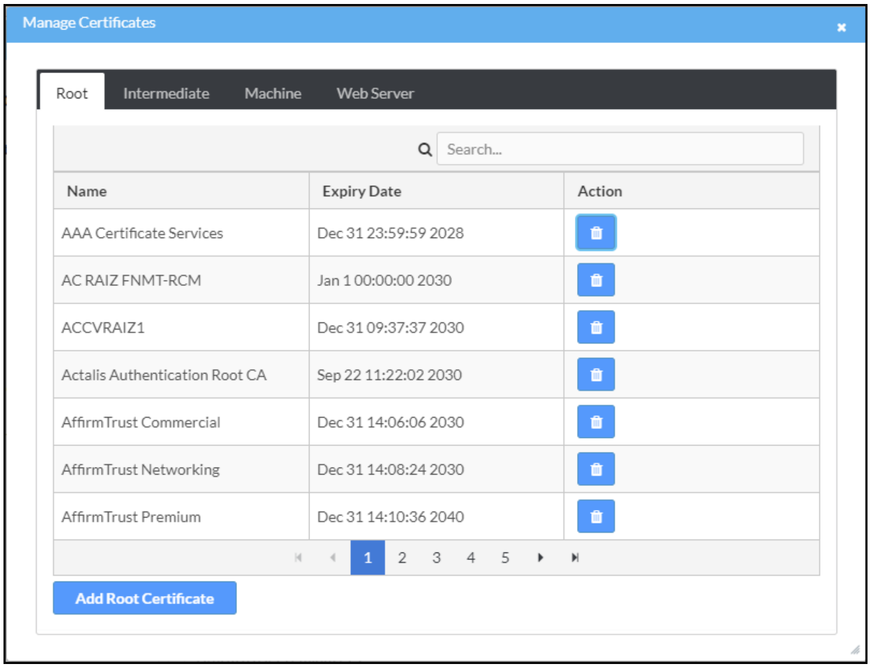
Download Logs

Download log files for diagnostic purposes. The log files are stored in a compressed .tgz file, extract the log files to view them.

To download logs, select **Download Logs**.

Manage Certificates

Click **Manage Certificates** in the **Action** drop-down menu to add, remove and manage certificates used in 802.1x and other protected networks. The following certificate tabs are displayed:



Name	Expiry Date	Action
AAA Certificate Services	Dec 31 23:59:59 2028	🗑
AC RAIZ FNMT-RCM	Jan 1 00:00:00 2030	🗑
ACCVRAIZ1	Dec 31 09:37:37 2030	🗑
Actalis Authentication Root CA	Sep 22 11:22:02 2030	🗑
AffirmTrust Commercial	Dec 31 14:06:06 2030	🗑
AffirmTrust Networking	Dec 31 14:08:24 2030	🗑
AffirmTrust Premium	Dec 31 14:10:36 2040	🗑

Root

The Root certificate is used by the device to validate the network's authentication server. The device has a variety of Root certificates, self-signed by trusted CAs (Certificate Authorities), and preloaded into the device. Root certificates must be self-signed.

To add a Root certificate:

1. Select the **Root** tab.
2. Click **Add Root Certificate**.
3. Select the certificate file from the dialog box that is displayed and click **Open**.

Intermediate

The Intermediate store holds non self-signed certificates that are used to validate the authentication server. These certificates will be provided by the network administrator if the network does not use self-signed Root certificates.

To add an Intermediate certificate:

1. Select the **Intermediate** tab.
2. Click **Add Intermediate Certificate**.
3. Select the certificate file from the dialog box that is displayed and click **Open**.

Machine

The machine certificate is an encrypted PFX file that is used by the authentication server to validate the identity of the device. The machine certificate will be provided by the network administrator, along with the certificate password. For 802.1x, only one machine certificate can reside on the device.

To add a Machine certificate:

1. Select the **Machine** tab.
2. Click **Add Machine Certificate**.
3. Select the certificate file from the dialog box that is displayed and click **Open**.

Web Server

The Web Server certificate is a digital file that contains information about the identity of the web server.

To add a Web Server certificate:

1. Select the **Web Server** tab.
2. Click **Add Web Server Certificate**.
3. Select the certificate file from the dialog box that is displayed and click **Open**.

Save Changes

The **Action** drop-down menu changes into a **Save Changes** drop-down menu when there are changes that can be saved.

To save configuration setting changes, select **Save Changes**.

Revert

To discard configuration settings changes, select **Revert**.

Log Out

To log out from the web configuration and return to the welcome screen, click 👤 > **Sign Out**.

This page is intentionally left blank.

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

Product Manual — Doc. 8661A
(2056508)
06/23/21
Specifications subject to
change without notice.