

# Installation, Operation, and Configuration

## Table of Contents

<b>Introduction.....</b>	<b>2</b>	<b>Installing and Replacing a Local Antenna ....</b>	<b>18</b>
Qualified Persons.....	2	Installing Local Antenna 904-002450-02 .....	18
Read this Instruction Sheet.....	2	Replacing a Local Antenna .....	18
Retain this Instruction Sheet.....	2	<b>Configuring the Communications Gateway... 19</b>	
Video .....	2	Software User's Guide.....	19
Proper Application .....	2	General Status.....	23
Warranty.....	3	Gateway Settings .....	24
<b>Safety Information.....</b>	<b>4</b>	Device Management.....	45
Understanding Safety-Alert Messages .....	4	TripSaver® II Service Center	
Following Safety Instructions .....	4	Configuration Software .....	47
Replacement Instructions and Labels .....	4	Remote Drop Open .....	49
Location of Safety Labels.....	5	Gang/Local Operation .....	52
<b>Safety Precautions .....</b>	<b>6</b>	DNP3 Master Settings .....	56
<b>Shipping and Handling.....</b>	<b>7</b>	DNP3 Outstation Settings .....	58
Packing .....	7	User Roles.....	68
Inspection.....	7	Security Settings.....	70
Handling .....	7	Profile .....	75
Storage .....	7	Diagnostics .....	76
Returning .....	7	<b>Commissioning (Pairing) a</b>	
<b>Mounting, Powering, and Securing the</b>		<b>TripSaver II Recloser for Use with the</b>	
<b>Communications Gateway.....</b>	<b>8</b>	<b>Communications Gateway.....</b>	<b>78</b>
Mounting the Communications Gateway to		Service Center Pairing a TripSaver II Recloser	
a Pole.....	9	with Firmware Version 1.8 or Later.....	78
Powering the Communications Gateway .....	10	Field Pairing a TripSaver II Recloser with	
Securing the Communications Gateway.....	11	Firmware Version 1.6 or 1.7 Installed on the	
<b>Installing and Replacing a Radio .....</b>	<b>12</b>	Utility Pole and Powered by Line Current .....	79
Installing a New Radio.....	12	<b>Troubleshooting.....</b>	<b>81</b>
Replacing a Radio .....	13	Signal Interference.....	81
<b>Installing and Replacing a Backup Battery ... 14</b>		Pairing Process Takes Longer Than Expected .....	81
Installing a New Battery.....	14	<b>Quick Installation Checklist.....</b>	<b>82</b>
Replacing a Battery.....	15	<b>Appendix A .....</b>	<b>83</b>
<b>Installing Remote Antenna Kits.....</b>	<b>16</b>	Interface Pinouts.....	83
Installing Remote Antenna Kit		Power System Diagram.....	84
903-002702-02/01 .....	16	Understanding the Radio Mode .....	85
Installing Remote Antenna Kit		Gateway Controller Module Indicator Lights .....	87
903-002701-01/02 .....	17	<b>Appendix B .....</b>	<b>88</b>
Installing Remote Antenna Kit		Regulatory Information .....	88
903-002700-02/03 .....	17		



## Qualified Persons

### **WARNING**

Only qualified persons who are knowledgeable in the installation, operation, and maintenance of overhead and underground electric distribution equipment, along with all associated hazards, may install, operate, and maintain the equipment covered by this publication. A qualified person is someone who is trained and competent in:

- The skills and techniques necessary to distinguish exposed live parts from nonlive parts of electrical equipment
- The skills and techniques necessary to determine the proper approach distances corresponding to the voltages to which the qualified person will be exposed
- The proper use of special precautionary techniques, personal protective equipment, insulated and shielding materials, and insulated tools for working on or near exposed energized parts of electrical equipment

These instructions are intended only for such qualified persons. They are not intended to be a substitute for adequate training and experience in safety procedures for this type of equipment.

## Read this Instruction Sheet

### **NOTICE**

Thoroughly and carefully read this instruction sheet before installing, operating or configuring a TripSaver II Communications via Gateway system. The latest version is available online in PDF format at [sandc.com/en/support/product-literature/](http://sandc.com/en/support/product-literature/). Become familiar with Safety Information on page 4 and Safety Precautions on page 6.

## Retain this Instruction Sheet

This instruction sheet should be available for reference wherever the TripSaver II Communications via Gateway system is used. Retain this instruction sheet in a location where users can easily retrieve and refer to it.

## Video

A video about how to pair a communications gateway with a TripSaver II Cutout-Mounted Recloser is available at [sandc.com/GatewayPairing-video](http://sandc.com/GatewayPairing-video). The goal of the video is to provide a clear and simple visual reference. In no way is the video meant as a complete replacement of these written instructions.

## Proper Application

### **WARNING**

The equipment in this publication is only intended for a specific application. The application must be within the ratings furnished for the equipment. Ratings for the TripSaver® II Communications Gateway are listed in Specification Bulletin 461-33. The ratings are also on the S&C nameplate affixed inside the product.

The operating temperature range for the Communications Gateway is -40°C to +50°C (-40°F to +122°F).

### Warranty

The warranty and/or obligations described in S&C's standard conditions of sale, as set forth in Price Sheet 150, plus any special warranty provisions, as set forth in the applicable product-line specification bulletin, are exclusive. The remedies provided in the former for breach of these warranties shall constitute the immediate purchaser's or end user's exclusive remedy and a fulfillment of all the seller's liability. In no event shall the seller's liability to the immediate purchaser or end user exceed the price of the specific product that gives rise to the immediate purchaser's or end user's claim. All other warranties, whether express or implied or arising by operation of law, course of dealing, usage of trade or otherwise, are excluded. The only warranties are those stated in Price Sheet 150, and THERE ARE NO EXPRESS OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. ANY EXPRESS WARRANTY OR OTHER OBLIGATION PROVIDED IN PRICE SHEET 150 IS GRANTED ONLY TO THE IMMEDIATE PURCHASER AND END USER, AS DEFINED THEREIN. OTHER THAN AN END USER, NO REMOTE PURCHASER MAY RELY ON ANY AFFIRMATION OF FACT OR PROMISE THAT RELATES TO THE GOODS DESCRIBED HEREIN, ANY DESCRIPTION THAT RELATES TO THE GOODS, OR ANY REMEDIAL PROMISE INCLUDED IN PRICE SHEET 150.

## Safety Information

---

### Understanding Safety-Alert Messages

Several types of safety-alert messages may appear throughout this instruction sheet and on labels attached to crate, packing, and equipment. Become familiar with these types of messages and the importance of these various signal words:

#### **DANGER**

“DANGER” identifies the most serious and immediate hazards that will likely result in serious personal injury or death if instructions, including recommended precautions, are not followed.

#### **WARNING**

“WARNING” identifies hazards or unsafe practices that can result in serious personal injury or death if instructions, including recommended precautions, are not followed.

#### **CAUTION**

“CAUTION” identifies hazards or unsafe practices that can result in minor personal injury if instructions, including recommended precautions, are not followed.

#### **NOTICE**

“NOTICE” identifies important procedures or requirements that can result in product or property damage if instructions are not followed.

### Following Safety Instructions

If any portion of this instruction sheet is not understood and assistance is required, contact the nearest S&C Sales Office or S&C Authorized Distributor. Their telephone numbers are listed on S&C’s website [sandc.com](http://sandc.com), or call the S&C Global Support and Monitoring Center at 1-888-762-1100.

#### **NOTICE**

Read this instruction sheet thoroughly and carefully before installing the TripSaver II Communications via Gateway system.

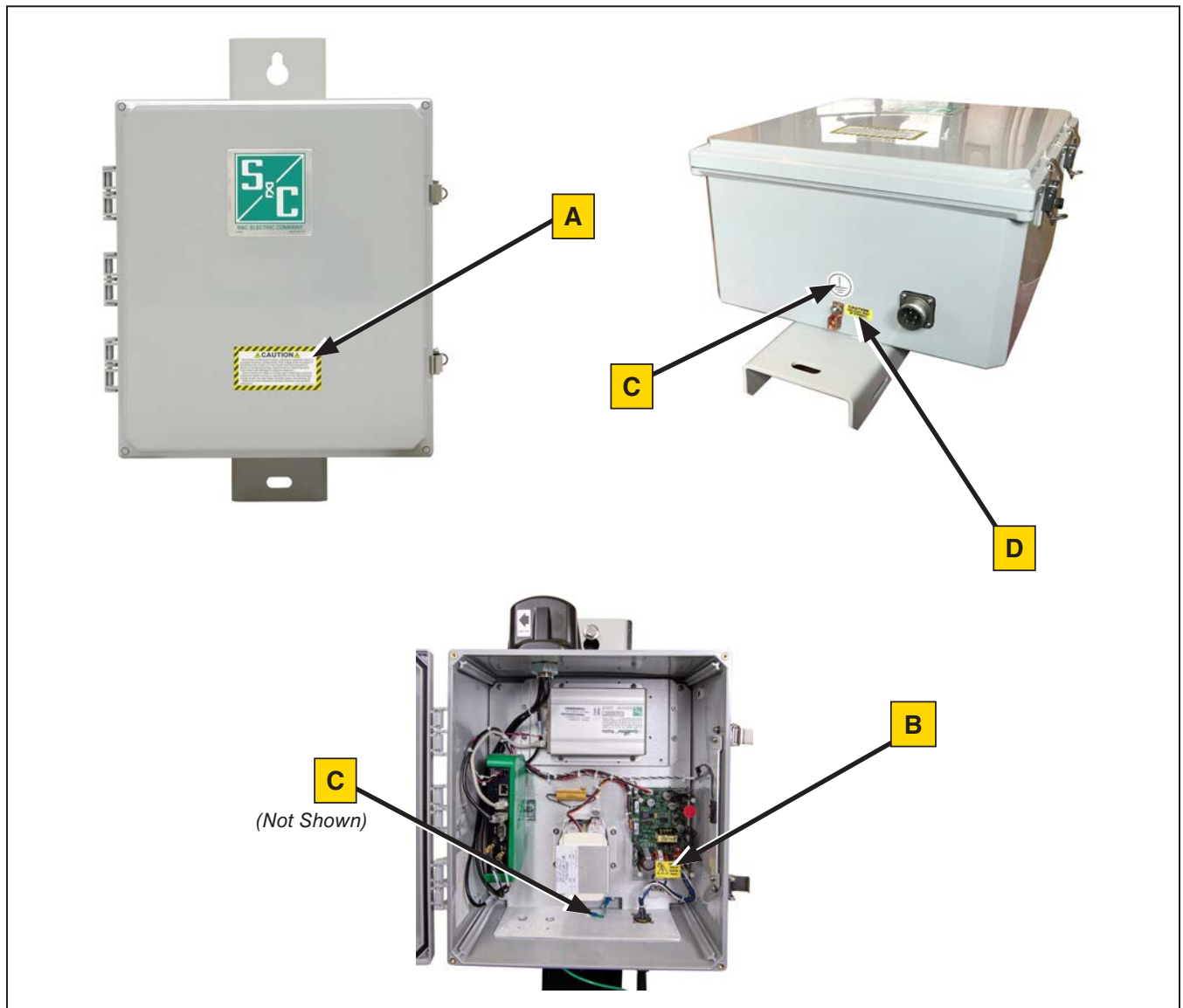


### Replacement Instructions and Labels

If additional copies of this instruction sheet are needed, contact the nearest S&C Sales Office, S&C Authorized Distributor, or S&C Headquarters. This instruction sheet can be downloaded from S&C’s website [sandc.com](http://sandc.com), or call the S&C Global Support and Monitoring Center at 1-888-762-1100.

It is important that any missing, damaged, or faded labels on the equipment be replaced immediately. Replacement labels are available by contacting the nearest S&C Sales Office, S&C Authorized Distributor, or S&C Headquarters.

Location of Safety Labels



Reorder Information for Safety Labels

Location	Safety Alert Message	Description	Part Number
A	<b>⚠ CAUTION</b>	This control is connected to electrical distribution equipment...	180-000070-00 Rev A
B	<b>⚠ CAUTION</b>	Risk of electric shock...	180-002533-01
C	<b>⚠ CAUTION</b>	Earth Ground	180-002577-01
D	<b>⚠ CAUTION</b>	Enclosure must be grounded...	180-000710-01

## Safety Precautions

### DANGER



The TripSaver II Communications via Gateway system connects to a 120/240-Vac source. Failure to observe these precautions will result in serious personal injury or death.

Some of these precautions may differ from your company's operating procedures and rules. Where a discrepancy exists, follow your company's operating procedures and rules.

1. **QUALIFIED PERSONS.** Access to a TripSaver II Communications via Gateway system must be restricted only to qualified persons. See the "Qualified Persons" section on page 2.
2. **SAFETY PROCEDURES.** Always follow safe operating procedures and rules.
3. **PERSONAL PROTECTIVE EQUIPMENT.** Always use suitable protective equipment, such as rubber gloves, rubber mats, hard hats, safety glasses, and flash clothing, in accordance with safe operating procedures and rules.
4. **SAFETY LABELS.** Do not remove or obscure any of the "DANGER," "WARNING," "CAUTION," or "NOTICE" labels. Remove tags ONLY if instructed to do so.
5. **ENERGIZED COMPONENTS.** Always consider all parts live until de-energized, tested, and grounded.
6. **MAINTAINING PROPER CLEARANCE.** Always maintain proper clearance from energized components.

## Packing

A complete TripSaver II Communications via Gateway system for a new installation consists of two shipping containers. They include the following:

- The communications gateway (including radio, if specified “factory-furnished” at time of order), an optional battery if specified, and mounting hardware for securing the enclosure to the pole
- (Optional) An ac power cable

## Inspection

Examine the shipment for external evidence of damage as soon after receipt as possible, preferably before removal from the carrier’s conveyance. Check the bill of lading to make sure the listed shipping containers are present.

If there is visible loss and/or damage:

1. Notify the delivering carrier immediately.
2. Ask for a carrier inspection.
3. Note the condition of shipment on all copies of the delivery receipt.
4. File a claim with the carrier.

If concealed damage is discovered:

1. Notify the delivering carrier within 15 days of receipt of shipment.
2. Ask for a carrier inspection.
3. File a claim with the carrier.

Also, notify S&C Electric Company in all instances of loss and/or damage.

## Handling

### CAUTION

**DO NOT** drop the communications gateway or subject any of its parts to undue stress during installation. Only remove the communications gateway from the carton when you are ready for installation. The communications gateway weighs about 25 lbs. (11.3 kg); follow proper lifting techniques to avoid minor injury.

## Storage

TripSaver II Communications Gateways are shipped on pallets banded with plastic wrap. This packaging is designed to protect the communications gateway from freight damage. This packaging is not suitable for outdoor storage because it can pool water and damage the communications gateway. After receipt, TripSaver II Communications Gateways should be stored indoors in their shipping packaging. Storing communications gateways outdoors in the shipping packaging will void the warranty.

## Returning

If for any reason the communications gateway is to be returned, place it in the original shipping carton to prevent damage during shipping. If additional shipping cartons are required, contact the nearest S&C Sales Office, S&C Authorized Distributor, or S&C Headquarters.



# Mounting, Powering, and Securing the Communications Gateway

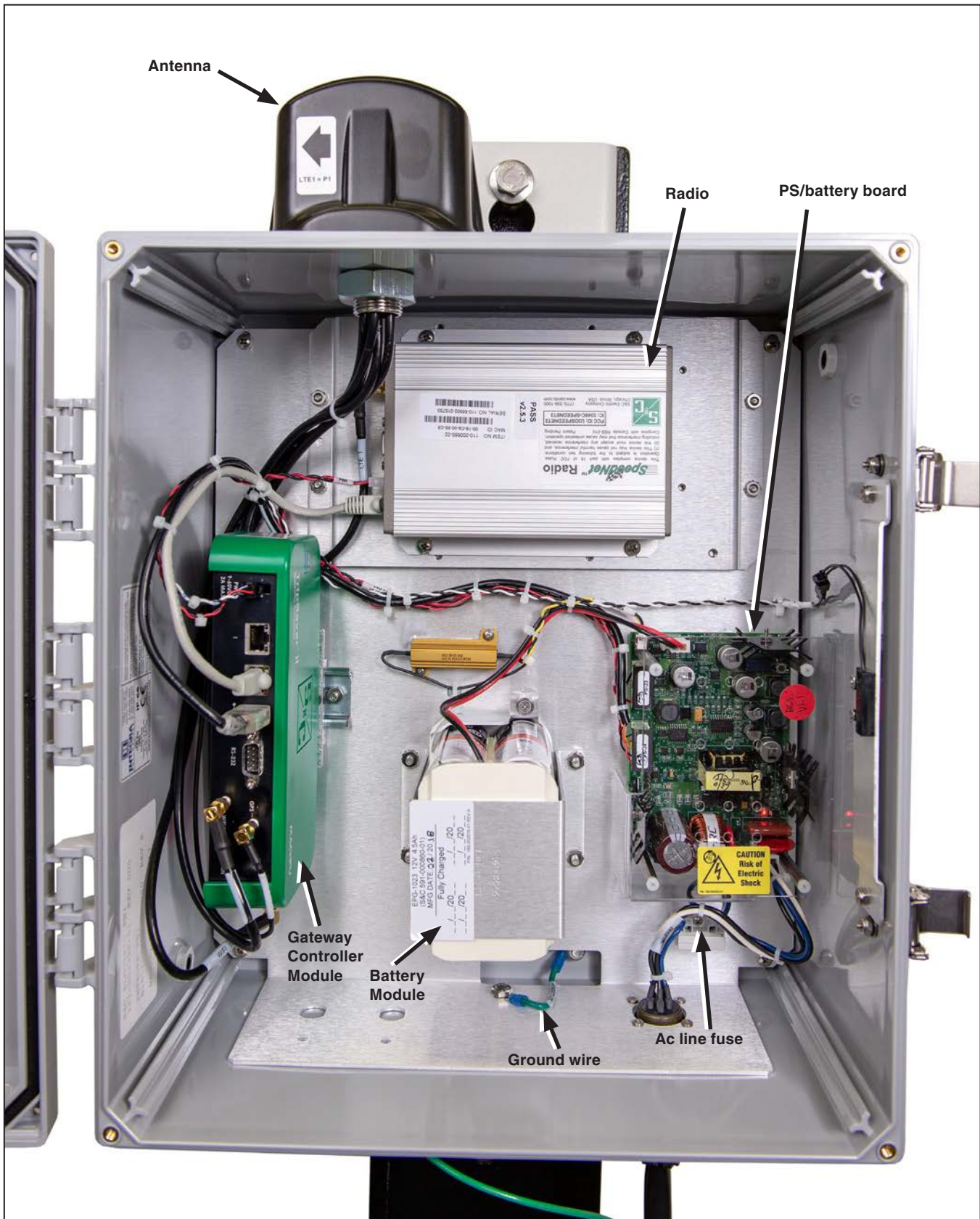


Figure 1. The TripSaver II Communications Gateway.



## Mounting the Communications Gateway to a Pole

Follow these steps to mount the communications gateway:

- STEP 1.** Attach the communications gateway in an upright position, with the S&C logo facing you, to the pole using the upper and lower mounting bolts provided. See Figure 2.
- STEP 2.** Connect a #2 copper (or equivalent) ground wire from the base of the communications gateway to the ground rod.

The communications gateway antenna is directional. The communications gateway should be mounted ideally no more than 30 feet (9.1 m) below the TripSaver II reclosers to which it will be paired. There should be an unobstructed line of sight between the gateway antenna and the LCD screen of each TripSaver II recloser. S&C recommends mounting the communications gateway directly beneath and on the same side of the pole as the reclosers to which it will be paired. Do not mount the gateway perpendicular to the TripSaver II reclosers or on the opposite side of the pole.



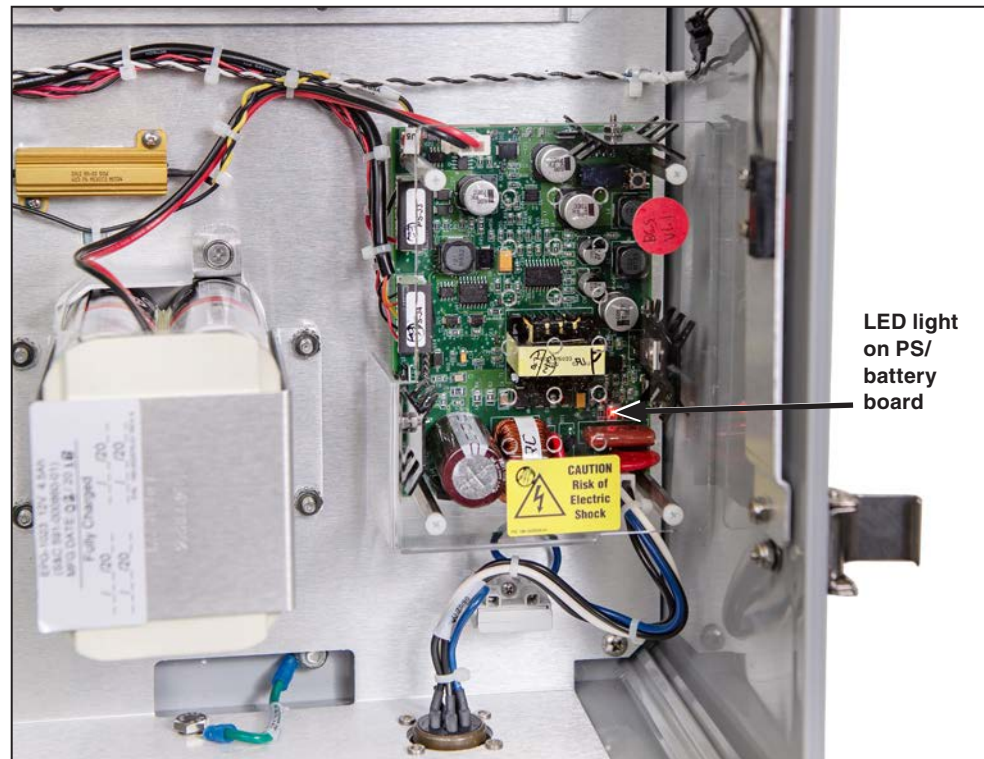
Figure 2. Mounting the communications gateway to the utility pole

## Mounting, Powering, and Securing the Communications Gateway

### Powering the Communications Gateway●

Follow these steps to power the communications gateway:

- STEP 1.** Remove the red protection cap attached to the power-connection terminal at the bottom of the communications gateway.
- STEP 2.** Run the ac power cable down the pole. The unterminated end of the cable should be connected to the overhead transformer.
- STEP 3.** Align the five-pin connector at the terminated end with the notch of the power connection terminal, make the connection, and tighten the ring. See Figure 2 on page 9.
- STEP 4.** Open the box.
- STEP 5.** After a short delay, LEDs on the PS/battery board and the gateway controller should light up, indicating the communications gateway is receiving power. See Figure 1 on page 8 and Figure 3.



**Figure 3. The communications gateway control PS/battery board.**

- A user-supplied disconnect switch may be required for installation between the ac input and the PS/battery board. Contact the nearest S&C Sales Office for details. See the power system diagram (Figure 76 on page 84).

### Securing the Communications Gateway

Follow these steps to secure the communications gateway:

- STEP 1.** Close the door and use the door latches to secure the enclosure. See Figure 2 on page 9.
- STEP 2.** The door latches accept locks with a maximum shackle diameter of  $\frac{3}{8}$ -inches (9.5 mm).

## Installing and Replacing a Radio

### Installing a New Radio

A radio providing field-area network capability for SCADA applications, if specified, is furnished factory-installed in the communications gateway. Alternately, the customer may install a user-furnished radio. See Figure 4.

Follow these steps to install a radio in the communications gateway:

- STEP 1.** Disconnect the ac power cable connected to the bottom of the gateway and then disconnect the ac line fuse located at the lower right corner of the gateway box.
- STEP 2.** Install the radio on the mounting plate using user-furnished hardware.
- STEP 3.** The wiring harness on most radios includes a power plug and data-port connectors (Ethernet or RS-232 serial). Insert the power plug in its receptacle. As applicable, connect the Ethernet connector to Port 2 of the green gateway controller or insert the serial connector in its receptacle on the gateway controller.

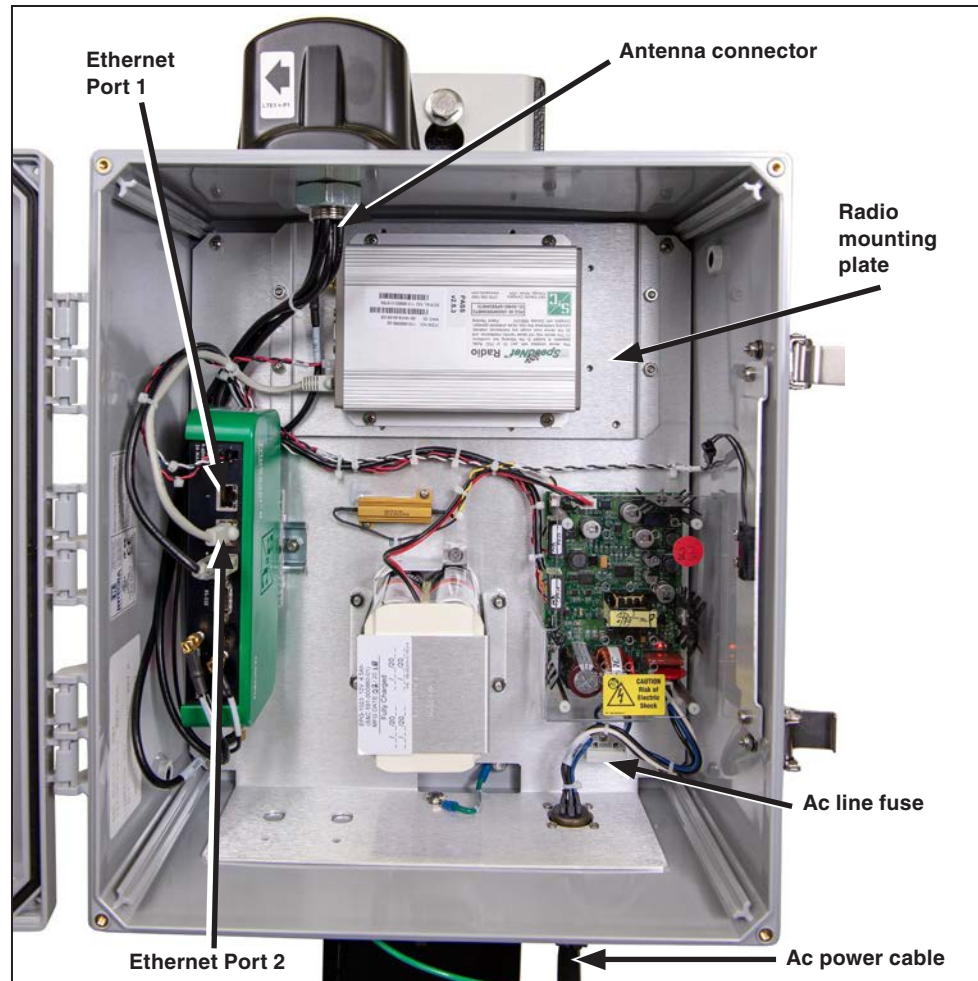


Figure 4. Installing a radio.

- STEP 4.** Attach the antenna connector to the user-furnished radio. If using the standard S&C-provided antenna, the applicable leads are LTE 1 (890- to 960-MHz/1710- to 2700-MHz bands) and LTE 2 (diversity). If using a remote antenna, use the leads from the surge-suppressor connector. Refer to the “Installing Remote Antenna Kits” section on page 16 for further information.

**Note:** Radios may be pre-programmed or may need to be programmed via a physical cable or over the air. When programming via a physical cable, if the radio is already installed in the gateway box, remove the radio-tray assembly so the cable connection to the radio becomes easier. When programming is complete, reinstall the radio-tray assembly and replace and securely tighten the four  $\frac{1}{8}$ -inch bolts.

- STEP 5.** Replace the ac line fuse located at the lower right corner of the gateway box. Reconnect the ac cable connector.

### Replacing a Radio

Follow these steps to replace a radio in the gateway:

- STEP 1.** Disconnect the ac power cable connected to the bottom of the gateway and then disconnect the ac-line fuse located at the lower right corner of the gateway box. See Figure 4 on page 12.

- STEP 2.** Remove the existing field-area network radio. See Figure 4 on page 12.

- (a) Disconnect the power plug from its receptacle.
- (b) As applicable, disconnect the Ethernet connector or the serial connector from the receptacles on the radio.
- (c) Disconnect the antenna connector.
- (d) Remove the radio from the mounting plate.

- STEP 3.** Install the new radio. Follow the procedure outlined in the “Installing a New Radio” section on page 12.

**Note:** S&C recommends the new radio be programmed before installation to match the configuration of the previous radio.

- STEP 4.** Replace the ac line fuse located at the lower right corner of the gateway box. Reconnect the ac cable connector.

## Installing and Replacing a Backup Battery

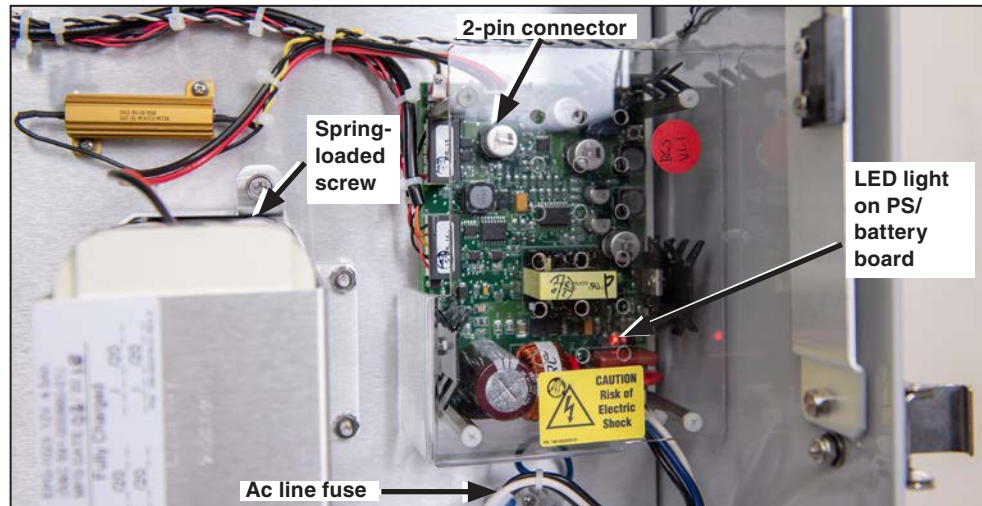
### Installing a New Battery

A backup battery to support the loss of control power and the gang operation feature, if specified, is furnished factory-installed in the communications gateway. For customers who initially choose not to have a backup battery, a backup battery system kit (903-002460-01) can be retrofitted to the communications gateway. See Figure 5 and Figure 6 on page 15.

Follow these steps to install the battery in the communications gateway:

**STEP 1.** Disconnect the ac power cable connected to the bottom of the gateway and then disconnect the ac-line fuse located at the lower right corner of the gateway box. See Figure 4 on page 12.

**STEP 2.** Install the battery. The battery kit includes a battery, a top bracket, and hardware.



**Figure 5.** Disconnect the Ac line fuse and install the battery.

- (a) The battery should be installed in the lower-middle section of the gateway.
- (b) Install the battery using the two spring-loaded screws, with the connector facing outward on top.
- (c) Install the top bracket using the four nuts.

**STEP 3.** Connect the battery.

With the ac line fuse still removed, connect the red and black battery leads to the white 2-pin connector on the PS/battery board. The acrylic safety cover over the PS/battery board does not need to be removed to make this connection.

**STEP 4.** With the ac line fuse still removed, reconnect the ac cable connector.

**STEP 5.** Check the LEDs on the green gateway controller. After a short delay, LEDs on the gateway controller should light up. This indicates the battery is functioning.

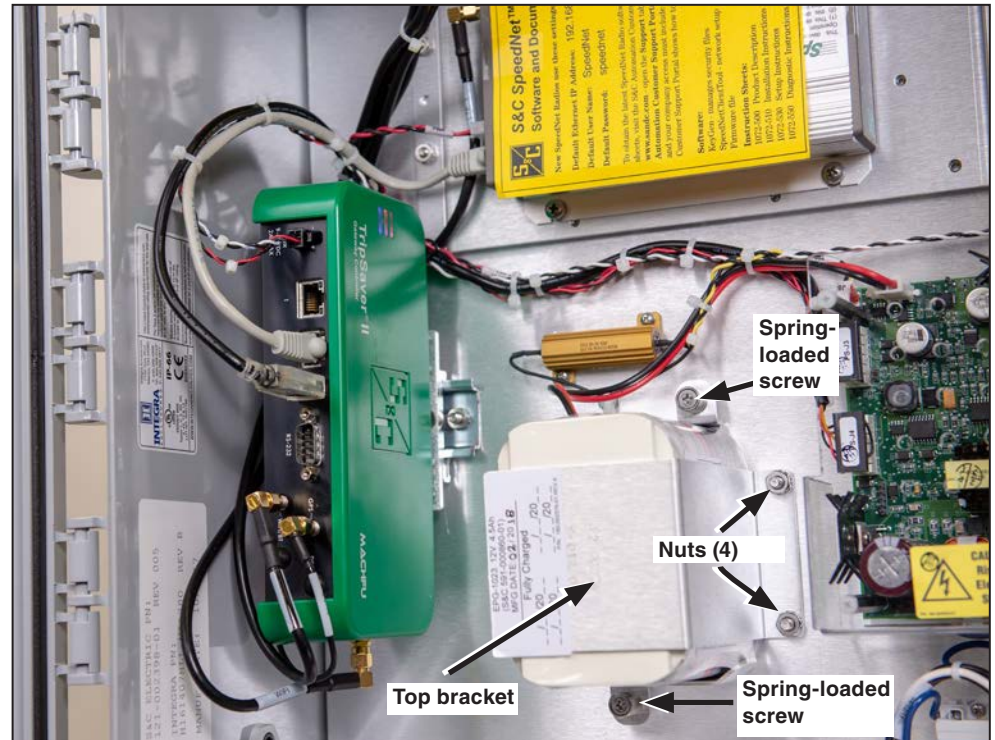
**STEP 6.** Disconnect the ac cable connector.



**STEP 7.** Replace the ac line fuse.

**STEP 8.** Reconnect the ac-cable connector.

**Note:** There is a jumper inside the external ac cable connector. This jumper was designed to avoid battery depletion during shipping. When the ac cable connector is unplugged, the dc is also disconnected because the jumper is not present, so the communications gateway does not receive any power.



**Figure 6.** Battery installation.

## Replacing a Battery

Follow these steps to replace a battery in the communications gateway:

**STEP 1.** Disconnect the ac power cable connected to the bottom of the gateway (See Figure 2 on page 9) and then disconnect the ac line fuse located at the lower right corner of the gateway box. See Figure 4 on page 12.

**STEP 2.** Remove the pre-installed battery located in the bottom-middle section of the enclosure. See Figure 6.

- Disconnect the red and black battery leads from white 2-pin connector on the PS/battery board. See Figure 5 on page 14.
- Unscrew the four nuts that hold the battery pack and top bracket in place.
- Loosen the two spring-loaded screws and remove the battery pack from the enclosure.

**STEP 3.** Install a new battery. Follow the procedure as outlined in the “Installing a New Battery” section on page 14.

## Installing Remote Antenna Kits

### Installing Remote Antenna Kit 903-002702-02/01

The 403- to 470-MHz, 2-dBi antenna kit includes an omnidirectional antenna with an N-male connector, pole mounting and bracket BM-1009, 2-shrink tubing, grounding kits for the LMR-400, and a weather-resistant cable tie. 40-foot (12.2-m) or 60-foot (18.3-m) coaxial cable length options are available.

Follow these steps to install Remote Antenna Kit 903-002702-02/01:

- STEP 1.** Install the antenna on the antenna bracket with one U-bolt. The white antenna mast should be above the bracket, with only the brass base clamped in the bracket.
- STEP 2.** Attach the antenna bracket to the pole. The pole should not block the line of sight to other antennas.
- STEP 3.** Slip the supplied cold-shrink tube over the antenna cable and connect the end where the shrink tube was applied to the antenna. Tighten finger-tight.
- STEP 4.** Wrap the cable connector inside the antenna with one piece of vinyl mastic tape. Don't stretch excessively, and do not block the antenna drain holes. See Figure 7.
- STEP 5.** Apply the second piece of tape overlapping the end of the first piece and tightly cover the cable end of the connector.
- STEP 6.** Align the end of the cold-shrink tube flush with the bottom of the antenna and shrink it over the tape and cable.
- STEP 7.** Tie-wrap the cable to the antenna bracket. Create a drip loop below the antenna. See Figure 8. Loop and secure any excess antenna cable near the pole. Use of a U-guard is recommended to protect the cables. Do not use staples. See Figure 8.
- STEP 8.** Slip a cold-shrink tube over the control end of the antenna cable and connect the cable to the surge suppressor at the bottom of communications gateway box. Waterproof this connector to industry standards.



Figure 7. Do not block antenna drain holes.

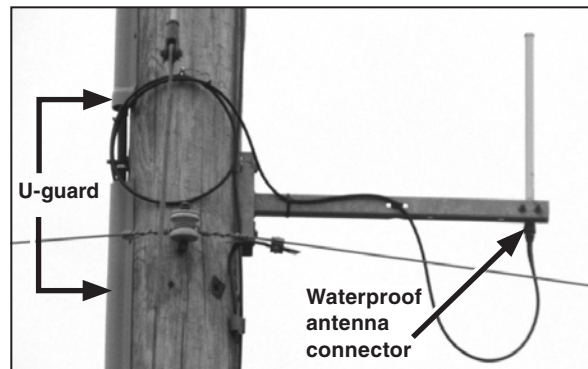


Figure 8. The remote antenna.

### Installing Remote Antenna Kit 903-002701-01/02

The 890- to 960-MHz, 10-dBi antenna includes an omnidirectional Yagi antenna, a pole-mounted single antenna arm with 30-foot (9.1-m) or 50-foot (15.2-m) coaxial cable, and N-type male connectors on both ends. The customer must provide 1.375-inch (35-mm) OD pipe for the antenna.

Follow these steps to install Remote Antenna Kit 903-002701-01/02:

- STEP 1.** Install the antenna on the antenna bracket.
- STEP 2.** Attach the antenna bracket to the pole to the specified azimuth, per the network design. The pole should not block the line of sight to other antennas.
- STEP 3.** Slip the supplied cold-shrink tube over the antenna cable and connect the end where the shrink tube was applied to the antenna. Tighten finger-tight.
- STEP 4.** Wrap the cable connector inside the antenna with one piece of vinyl mastic tape. Don't stretch excessively, and do not block the antenna drain holes.
- STEP 5.** Apply the second piece of tape overlapping the end of the first piece and tightly cover the cable end of the connector.
- STEP 6.** Align the end of the cold-shrink tube flush with the bottom of the antenna and shrink it over the tape and cable.
- STEP 7.** Tie-wrap the cable to the antenna bracket. Create a drip loop below the antenna. See Figure 8 on page 16. Loop and secure any excess antenna cable near the pole. Use of a U-guard is recommended to protect the cables. Do not use staples.
- STEP 8.** Slip a cold-shrink tube over the control end of the antenna cable and connect the cable to the surge suppressor at the bottom of communications gateway box. Waterproof this connector to industry standards.

### Installing Remote Antenna Kit 903-002700-02/03

The 902- to 928-MHz, 3-dBi antenna includes an omnidirectional fiberglass antenna, a pole-mounted single antenna arm with 30-foot (9.1-m) or 50-foot (15.2-m) coaxial cable and N-type male connectors on both ends.

Follow these steps to install Remote Antenna Kit 903-002700-02/03:

- STEP 1.** Install the antenna on the antenna bracket with one U-bolt.
- STEP 2.** Attach the antenna bracket to the pole. The pole should not block the line of sight to other antennas.
- STEP 3.** Slip the supplied cold-shrink tube over the antenna cable and connect the end where the shrink tube was applied to the antenna. Tighten finger-tight.
- STEP 4.** Wrap the cable connector inside the antenna with one piece of vinyl mastic tape. Don't stretch excessively, and do not block the antenna drain holes.
- STEP 5.** Apply the second piece of tape overlapping the end of the first piece and tightly cover the cable end of the connector.
- STEP 6.** Align the end of the cold-shrink tube flush with the bottom of the antenna and shrink it over the tape and cable.
- STEP 7.** Tie-wrap the cable to the antenna bracket. Create a drip loop below the antenna. See Figure 8 on page 16. Loop and secure any excess antenna cable near the pole. Use of a U-guard is recommended to protect the cables. Do not use staples.
- STEP 8.** Slip a cold-shrink tube over the control end of the antenna cable and connect the cable to the surge suppressor at the bottom of communications gateway box. Waterproof this connector to industry standards.

## Installing and Replacing a Local Antenna

---

### Installing Local Antenna 904-002450-02

The 403- to 470-MHz, 2-dBi antenna includes an omnidirectional antenna with an N-male connector.

- STEP 1.** Remove the protection cap attached to the antenna connector terminal at the bottom of the communications gateway box.
- STEP 2.** Screw in the antenna to the N-type female connector.
- STEP 3.** Waterproof the connector to industry standards.

### Replacing a Local Antenna

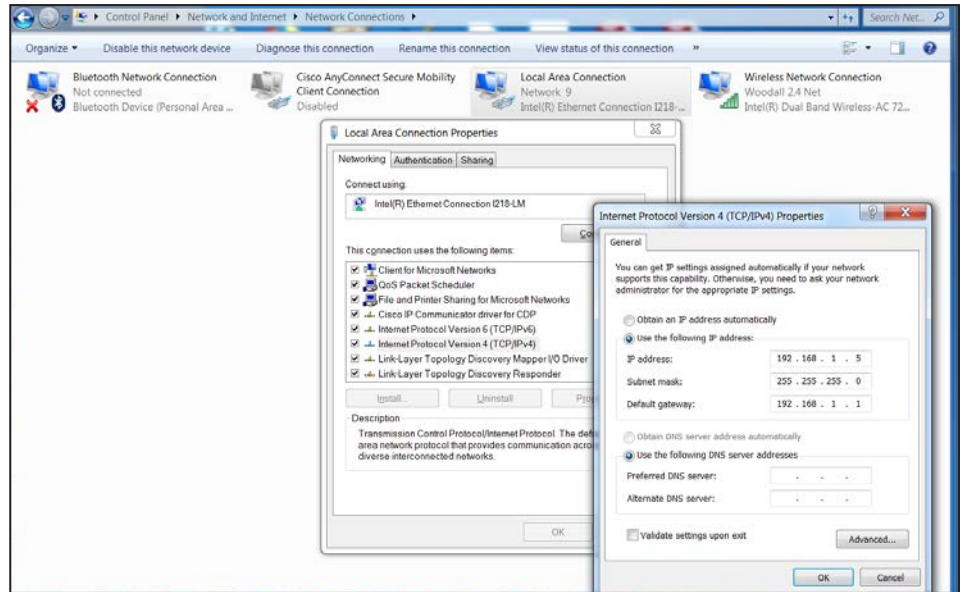
- STEP 1.** Visually inspect the antenna for damage (bent, not vertical)
- STEP 2.** If it needs to be replaced, remove any waterproofing material around the connector.
- STEP 3.** Unscrew the antenna.
- STEP 4.** Check to ensure the connector channel is clear.
- STEP 5.** Follow the procedure outlined in the previous section: “Installing Local Antenna.”

## Software User's Guide

### Logging on to the Communications Gateway

The communications gateway is accessed via a Web browser interface. Connect a PC with a CAT5 Ethernet cable to the communications gateway's Ethernet Port 1. See Figure 4 on page 12. The default configuration of the communications gateway's IP gateway is 192.168.1.1 with DHCP set as "On." To join the communications gateway network, set the PC's network address to "Obtain an IP Address Automatically" and "Obtain DNS Server Address Automatically" under the PC's LAN address settings to enable a network connection to the communications gateway. Alternately, a static IP address within the 192.168.1.x network may be used. See Figure 9.

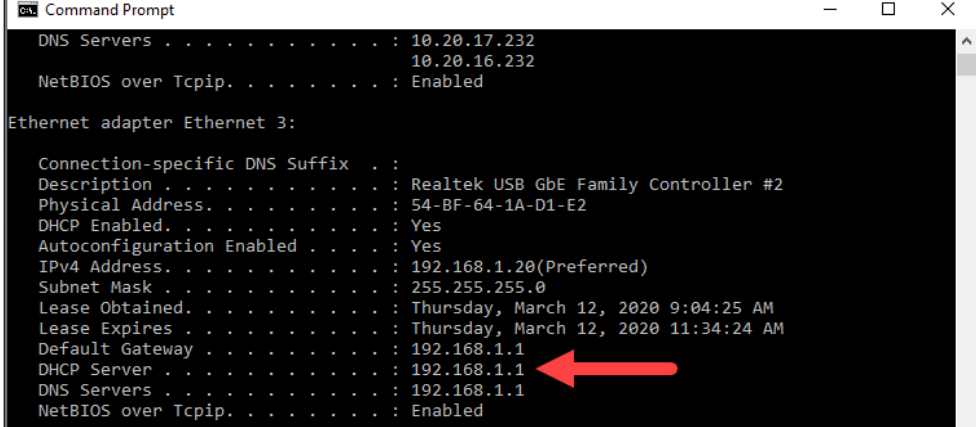
**Note:** To remove Windows routing conflicts, S&C recommends turning the PC's Wi-Fi radio off.



**Figure 9.** Setting a static IP address on the PC to connect to the communications gateway.

## Configuring the Communications Gateway

After allowing approximately 3 minutes for the gateway to boot, a confirmation the PC has successfully joined the communications gateway network may be observed by launching an MSDOS command window and running 'ipconfig /all' at the command prompt. An output showing all the IP interfaces for the host system will be displayed. Identify the Ethernet interface that has the cabled connection to communications gateway Ethernet Port 1 and examine the output for that interface. Screen information for the interface supporting a successful connection when using DHCP will resemble what's shown in Figure 10.



```
Command Prompt
DNS Servers . . . . . : 10.20.17.232
                    : 10.20.16.232
NetBIOS over Tcpi. . . . . : Enabled

Ethernet adapter Ethernet 3:

    Connection-specific DNS Suffix  . : 
    Description . . . . . : Realtek USB GbE Family Controller #2
    Physical Address. . . . . : 54-BF-64-1A-D1-E2
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IPv4 Address. . . . . : 192.168.1.20(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Thursday, March 12, 2020 9:04:25 AM
    Lease Expires . . . . . : Thursday, March 12, 2020 11:34:24 AM
    Default Gateway . . . . . : 192.168.1.1
    DHCP Server . . . . . : 192.168.1.1
    DNS Servers . . . . . : 192.168.1.1
    NetBIOS over Tcpi. . . . . : Enabled
```

Figure 10. A successful ipconfig/all reply from the Command prompt.



**Note:** If the interface indicates “media disconnected,” this is an indication the Ethernet connection between the host PC and the communications gateway is not functional, and it should be investigated.

### NOTICE

Because the end user can change the IP address range, or even disable DHCP completely and change the communications gateway to a static IP address, it is important to make a note of any IP settings changes. When relocating or setting up a communications gateway that has had its IP settings changed, look for the IP setting configured by your service or IT department when running ipconfig/all from the MSDOS command line.

With the CAT5 Ethernet cable attached to communications gateway’s Ethernet Port 1, launch a Web browser on the PC. Type 192.168.1.1 in the browser’s address line. (Browsers supported include Google Chrome, Internet Explorer, and Microsoft Edge.) The *Communications Gateway Login* screen will open with a username and password challenge. See Figure 11.

**Note:** The default username and password can be requested from S&C by calling the Global Support and Monitoring Center at 888-762-1100 or by contacting S&C through the S&C Customer Portal at [sandc.com/en/support/sc-customer-portal/](http://sandc.com/en/support/sc-customer-portal/).

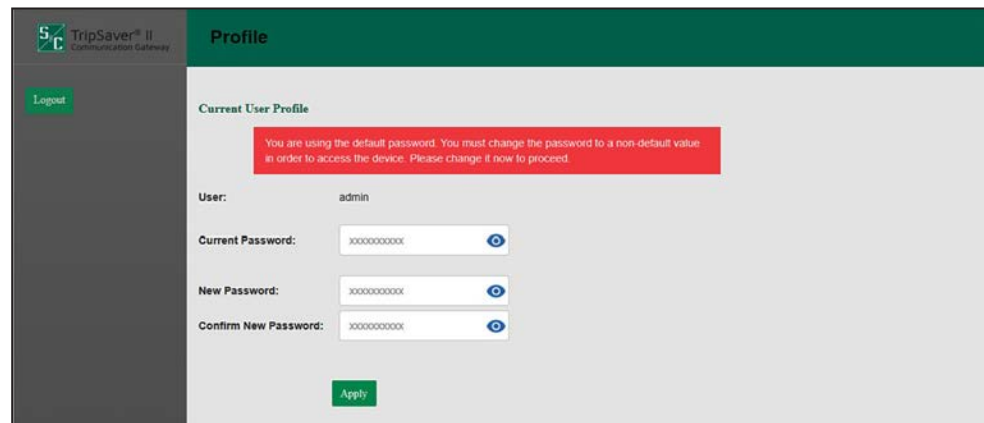


Figure 11. The *Communications Gateway Login* screen.

When logging in for the first time, users will be sent to the *Profile* screen and be prompted to change the default password.

### NOTICE

With communications gateway firmware version 3.1 and later, the default password for the admin user must be changed before proceeding. See Figure 12. The new non-default password must be at least 8 characters with at least one uppercase and one lowercase character. Numbers and special characters are also allowed but not required. <Space>, <Tab>, <&> characters are not allowed. Do not lose this password. There is no way to recover a lost password in the field. A lost password will require returning the gateway controller module to S&C for re-initialization.



The screenshot shows the 'Profile' screen of the TripSaver II Communication Gateway. The page title is 'Profile'. On the left, there is a 'Logout' button. The main content area is titled 'Current User Profile' and contains a red warning message: 'You are using the default password. You must change the password to a non-default value in order to access the device. Please change it now to proceed.' Below the warning, there are three password fields: 'User:' with the value 'admin', 'Current Password:' with a masked password 'xxxxxxxxxx', 'New Password:' with a masked password 'xxxxxxxxxx', and 'Confirm New Password:' with a masked password 'xxxxxxxxxx'. Each password field has a blue eye icon to toggle visibility. At the bottom of the form is a green 'Apply' button.

Figure 12. The *Profile* screen for changing the default password.

After a successful login, the browser will open to the communications gateway *General Status* screen with an application navigation menu on the left side of the screen. The navigation menu will remain visible for all subordinate menu interface screens. See Figure 13 on page 23.

### NOTICE

Simultaneous access to the web user interface by multiple users is not officially supported. If it is desired to have multiple users logged in simultaneously, it is strongly recommended that only one of those users be assigned the admin role. It is also strongly recommended that only one of those users modify settings on the gateway. The other users should be performing read-only activities. Also, if two users are sharing a single username and the users attempt to log in at the same time, the older session will be silently logged out.

## General Status

The purpose of the *General Status* screen is informational and for display only. No edits are allowed. Field edits are permitted under respective menu sections where each field's purpose is defined.

The *General Status* screen is comprised of the “Gateway Identity,” “GPS,” “Gateway LAN,” “Gateway WAN,” “Gateway Hardware,” and “SCADA Communication” panels. The “Gateway Identity” panel contains five fields: **Gateway Name**, **Gateway Serial #**, **Gateway Software Version**, **Gateway App Version**, and **Gateway Platform Version**. The “GPS” panel contains five fields: **Status**, **Time Since last GPS Fix**, **Location**, **Satellites (In Use)**, and **System Time**. The “Gateway LAN” and “Gateway WAN” panels contain three fields each: **Link Status**, **IP Address**, and **Netmask**. The “Gateway Hardware” panel contains four fields: **Battery Present**, **Battery Health**, **Battery Voltage (Volts)**, and **Door Status**. The SCADA Communication panel contains the **IEC104 Communication Status** field. See Figure 13.

The screenshot shows the 'General Status' screen for TripSaver II. The interface includes a left-hand navigation menu with options like 'General Status', 'Gateway Settings', 'Device Management', and 'Diagnostics'. The main content area is divided into several panels:

- Gateway Identity:**
  - Gateway Name: Dnp3 Demo
  - Gateway Serial Number: M1001282
  - Gateway Software Version: 4.1.00335
  - Gateway App Version: 2023.09.18 12:56 CDT | 6416f61a2
  - Gateway Platform Version: 7.1.2-1.2.7.1
- GPS:**
  - Status: Available
  - Time Since Last GPS Fix: 00:00:00
  - Location: 42° 0' 14.11071" N 87° 40' 39.42917" W
  - Satellites (In Use): 12 (12)
  - System Time: Fri, 13 Oct 2023 12:58:29 GMT
- Gateway LAN:**
  - Link Status: Up
  - IP Address: 192.168.1.1
  - Netmask: 255.255.255.0
- Gateway WAN:**
  - Link Status: Up
  - IP Address: 192.168.52.1
  - Netmask: 255.255.255.0
- Gateway Hardware:**
  - Battery Present: Yes
  - Battery Health: Operational
  - Battery Voltage (Volts): 13.64
  - Door Status: Open

Figure 13. The *General Status* screen.

# Configuring the Communications Gateway

## Gateway Settings

The *Gateway Settings* screen contains the “Gateway Name,” “Ethernet 1 (LAN),” “Ethernet 2 (WAN),” “IEC104 Protocol,” “Time Synchronization Source,” “Gateway Configuration,” “Firmware Upgrade,” “Reboot Gateway” and “Ping Station” panels.

**Note:** For all field edits within each menu, the **Save** button must be clicked for field modifications to occur.

### Gateway Name

The Gateway Name panel allows unique naming of the communications gateway. The data from this field will be delivered to the SCADA master via a DNP3 Group 0 read.

Enter a user-defined name for the communications gateway and click on the **Save** button. Naming of the communications gateway is limited to 50 characters. S&C recommends an intuitive naming convention for the communications gateways. See Figure 14.

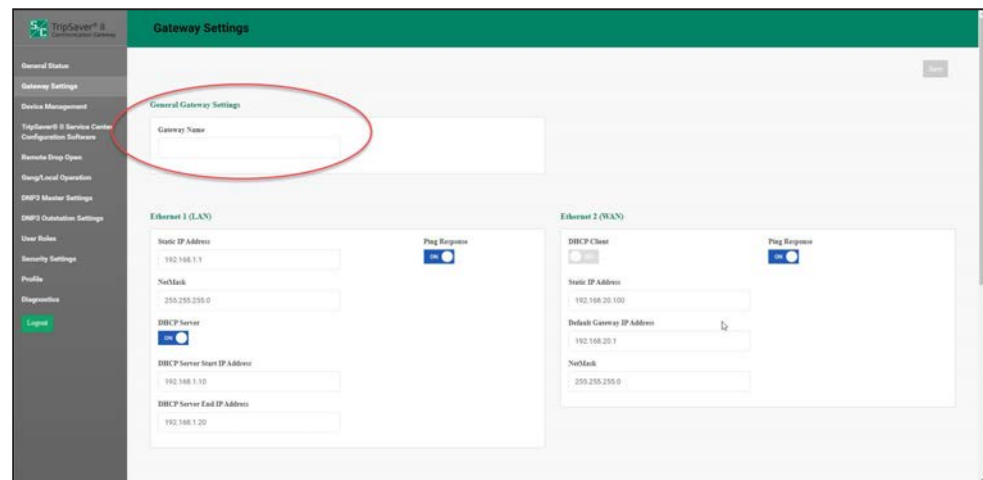


Figure 14. The Gateway Name field.

## Ethernet 1 (LAN)

In this panel, the network associated with the communications gateway local area network (LAN) is defined for management devices connecting to physical Ethernet Port 1. See Figure 15. As noted earlier, the communications gateway ships with a default IP address of 192.168.1.1, a NetMask equal to 255.255.255.0, and DHCP set to “On.” To modify these values for the communications gateway LAN, the fields that require identification are **Static IP Address**, **NetMask**, and **DHCP Server**.

**Note:** The **DHCP** toggle button either enables or disables dynamic host control protocol (DHCP) services on physical Ethernet Port 1.

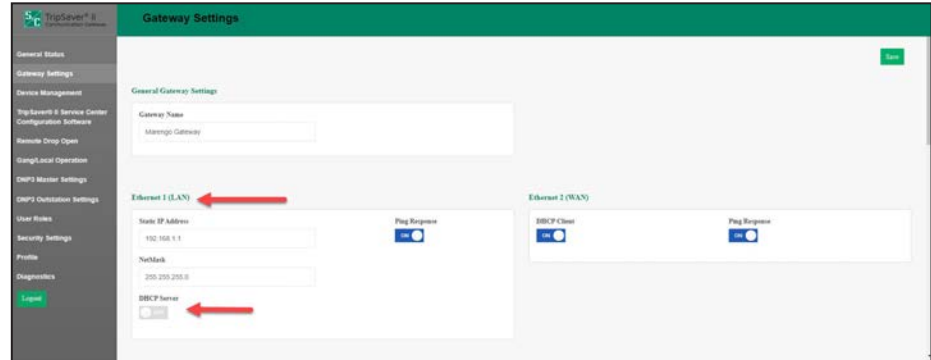


Figure 15. The Ethernet 1 (LAN) panel.

## Configuring the Communications Gateway

The fields required within this panel are determined by the **DHCP** button toggled to the **On** or **Off** positions. With DHCP in the **Off** position, management devices connected to communications gateway's physical Port 1 must be configured with a static IP address that resides in the communications gateway's LAN IP range identified by the NetMask setting in the previous field.

With DHCP in the **On** position, management devices connected to communications gateway's physical Port 1 will be assigned an IP address from the specified IP range determined by the **DHCP Server Start IP Address** and **DHCP Server End IP Address** fields. Also included is a **Ping Response** toggle button. Toggling this button to the **On** position will make the gateway responsive to a ping command. This toggle button is in the **Off** position by default. See Figure 16.

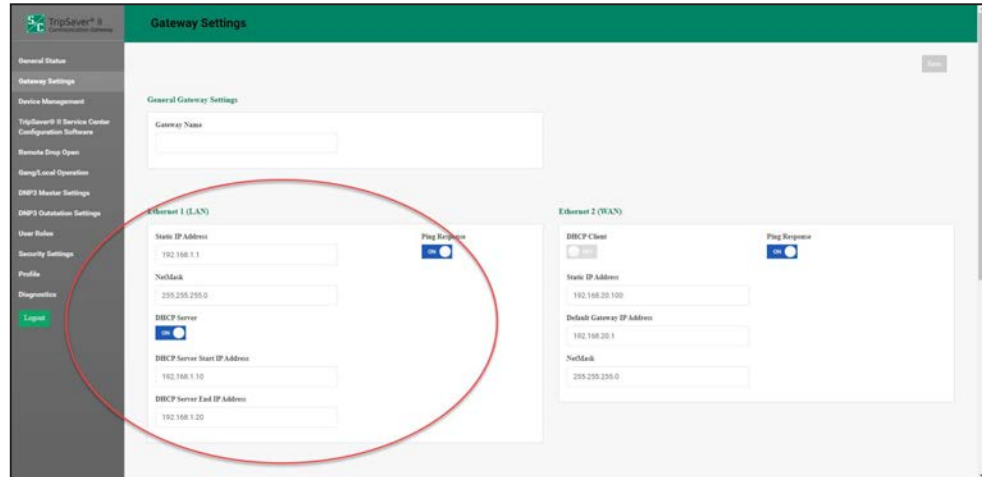


Figure 16. The Ethernet 1 (LAN) fields with DHCP set in the On position.



## Ethernet 2 (WAN)

This panel defines the IP addressing for the communications gateway's Ethernet Port 2 and subsequent network linkage and settings respective to the customer's legacy back-haul WAN network. See Figure 17.

**Note:** The use of these fields is for WANs that use Ethernet as a back-haul transport protocol. When serial is used for the back haul network, or there is no WAN, this panel will not require entries.

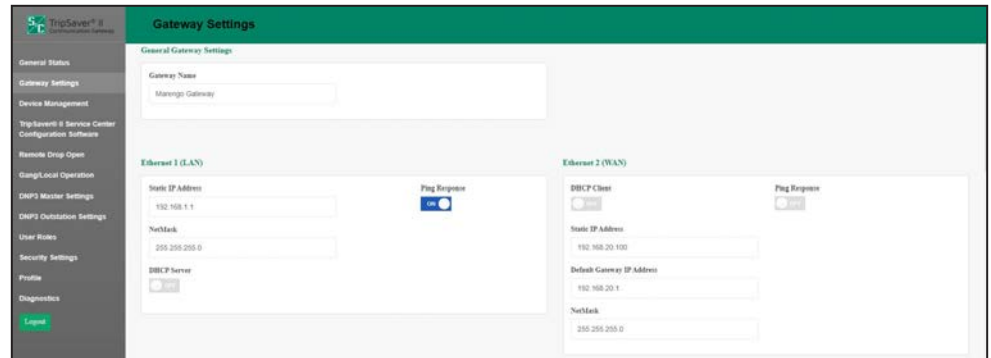


Figure 17. The Ethernet 2 (WAN) fields.

## DHCP State 'Off'

Three fields require identification: **Static IP Address**, **Default Gateway IP Address**, and **NetMask**. The **Static IP Address** field is the WAN IP address assigned to the communications gateway. The **Default Gateway IP Address** field is the address of the network device “up-stream” of the communications gateway and determines the destination of DNP3 traffic sent to the SCADA masters(s).

# Configuring the Communications Gateway

## DHCP State 'On'

No fields require identification. A DHCP request will be initiated by the communications gateway to the WAN's DHCP server, which will assign an IP address for all data communications over the WAN. See Figure 18.

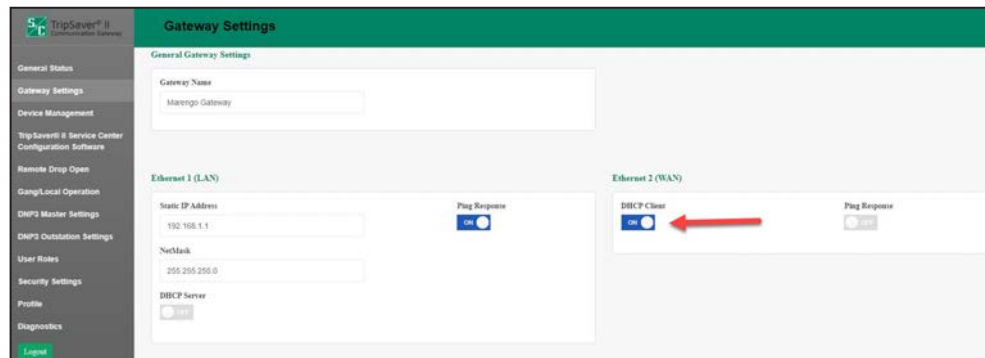
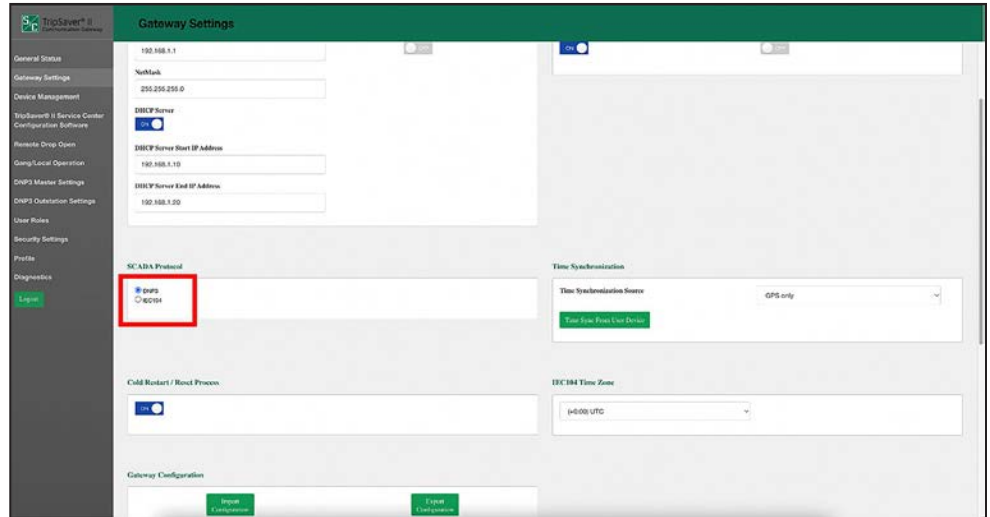


Figure 18. The Ethernet 2 (WAN) fields with DHCP set to the On position.

**Note:** For both the DHCP **On** and **Off** states, the **Ping Response** toggle button when toggled to the **On** position will make the gateway responsive to a ping command. This toggle button is in the **Off** position by default.

## SCADA Protocol

The communications gateway supports the use of the DNP3 protocol by default. It also supports the IEC 60870-5-104 protocol, or the “IEC104” protocol, which is a separate communications protocol from the DNP3 protocol. To switch to the IEC104 protocol, click on the **IEC104** button in the SCADA Protocol field, and then click on the **Save** button. See Figure 19.



**Figure 19.** The IEC104 Enable/Disable toggle button.

**Note:** Instructions for configuring the communications gateway using the IEC 60870-5-104, or “IEC104,” protocol are contained in S&C Instruction Sheet 461-519, “TripSaver® II Cutout-Mounted Recloser: Communications via Gateway using the IEC104 Protocol: *Installation, Operation, and Configuration.*”

**Note:** When enabling or disabling the IEC104 protocol, if settings have already been made with the communications gateway set to the DNP3 protocol, those settings will not be lost when the user enables IEC104, and vice versa.

## DNP3 Cold Restart/Reset Process

The **DNP3 Cold Restart/Reset** process allows the TripSaver II Communications Gateway to accept **DNP3 Cold Restart/Reset** commands from a SCADA master. The **DNP3 Cold Restart/Reset** process is user-configurable with the toggle on the web user interface and is disabled by default.

The **DNP3 Cold Restart/Reset** process provides the ability to remotely reset the DNP3 application services on the TripSaver II Communications Gateway platform. To address potential security concerns, the user-configurable **DNP3 Cold Restart/Reset Process** feature was added to the web user interface so the user could disable the **DNP3 Cold Restart/Reset** process when needed.

When the toggle is in the **Off** position, the TripSaver II Communications Gateway blocks the command from changing the DNP3 application services and sends a negative response to the SCADA master. When the toggle is in the **On** position, the TripSaver II Communications Gateway accepts the command and restarts the DNP3 application services. During the **Restart** process, the TripSaver II Communications Gateway is unable to respond to additional DNP3 requests.

## Time Synchronization

The communications gateway supports three primary methods of time synchronization: “GPS only,” “SCADA only,” and “GPS Primary, SCADA backup.” Select the desired option from the **Time Synchronization Source** drop-down menu and click the **Save** button. See Figure 20.

The communications gateway also supports a fourth method of time synchronization. To perform a one-time synchronization from the user’s computer that is accessing this Web interface, click on the **Time Sync From User Device** button. This will immediately sync the gateway’s clock to the time in the user’s computer. After this one-time synchronization, the gateway will continue to use its configured Time Synchronization Source to maintain its clock in the future. This option could be useful for lab purposes or for initial system deployment.

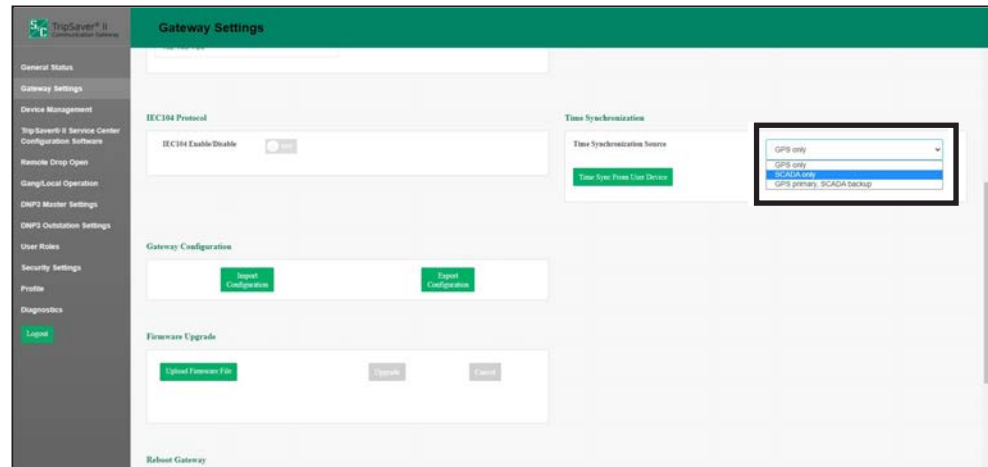


Figure 20. The Time Synchronization Source menu.

## Gateway Configuration

The communications gateway supports a capability to perform bulk imports and exports of certain configuration data parameters. The communications gateway will use the same XML file format for both import and export functions. This will allow a user to configure settings in one communications gateway device, export those settings into an XML file, and then import the same settings into another communications gateway. The selection of **Import Configuration** or **Export Configuration** options invokes a series of dialog boxes allowing navigation on a PC to a configuration file for “Import” or the saving of a file for “Export.” See Figure 21.

**Note:** When the IEC104 protocol is enabled, the export file will include all IEC104 settings and exclude all DNP3 settings. If DNP3 protocol is enabled, the export file will include all DNP3 settings and exclude all IEC104 settings.

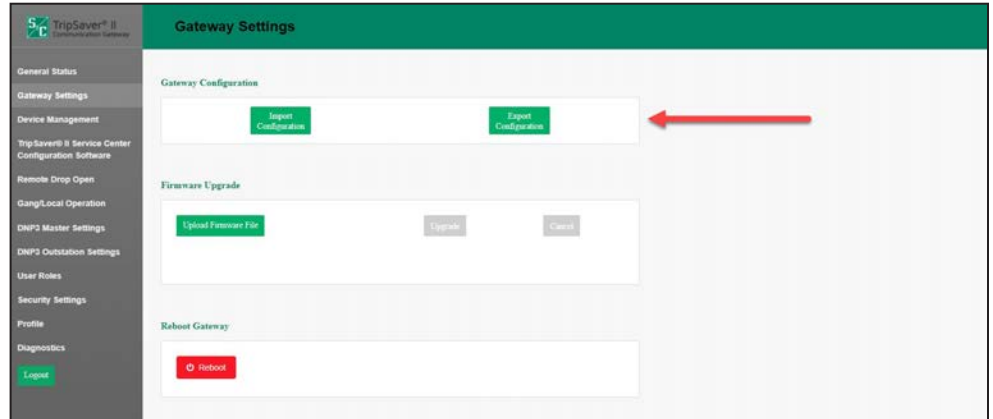


Figure 21. The Import Configuration and Export Configuration buttons.

## XML File Description

The XML file format is split into two sections. The first section is encapsulated by <ConfigDB> and <configuration> tags. Each item in this section is a simple name/value pair, for example:

```
<ConfigDB>
  <configuration>
    <item value="50" name="gatewayAddress"/>
  </configuration>
</ConfigDB>
```

where name="gatewayAddress" represents the communications gateway's own DNP3 address, and the associated value="50" is a simple integer. The list of parameters that can be included in the <ConfigDB> section of the XML is detailed in Table 1 on page 32.

# Configuring the Communications Gateway

**Table 1. Import and Export ConfigDB Parameters**

Name	Description	Data Type of Value	Range of Value
interface	Type of interface used for DNP3. See DNP3 Interface on <i>DNP3 Master Settings</i> screen.	String	TCP, UDP, Serial
serialBaud	Serial baud rate, used if interface=Serial. See Baud Rate on <i>DNP3 Master Settings</i> screen.	Integer	9600, 19200, 38400, 57600, 115200
serialStopBits	Serial stop bits, used if interface=Serial. See Stop Bits on <i>DNP3 Master Settings</i> screen.	Integer	1 or 2
serialParity	Serial parity, used if interface=Serial. See Parity on <i>DNP3 Master Settings</i> screen.	String	None, odd, even
serialFlow	Serial flow control, used if interface=Serial. See Flow Control on <i>DNP3 Master Settings</i> screen.	String	None, RTS/CTS, XON/XOFF
addressMode	DNP3 addressing mode. See Addressing Type on <i>DNP3 Outstation Settings</i> screen.	String	Concentrator
gatewayAddress	DNP3 address of gateway. See Gateway DNP3 Address on <i>DNP3 Outstation Settings</i> screen.	Integer	1 ... 65,519
tcpKeepAlive	See description for TCP Keepalive Timer on <i>DNP3 Outstation Settings</i> screen.	Integer	Any integer value
unsolicitedIndefiniteRetries	See description for Unsolicited Responses Retried Indefinitely on <i>DNP3 Outstations Settings</i> screen.	Boolean	0 (FALSE), 1 (TRUE)
unsolicitedResponsesToConfirm	See description for Number of Retries for Confirm on <i>DNP3 Outstation Settings</i> screen.	Integer	Any integer value
unsolicitedResponsesDelay	See description for Delay Before Retries on <i>DNP3 Outstation Settings</i> screen.	Integer	1 ... 300
disableObjectFlagCommLost	This setting disables the COMM_LOST flag in DNP3 standard Object Flags. When set to "true," the gateway disables the COMM_LOST flag so it will always be set to 0. When set to "false," the gateway conforms to the standard definition of COMM_LOST for DNP3 setpoints originating in the TripSaver II recloser. The usage of the COMM_LOST flag can cause frequent DNP3 events.	Boolean	True or False
dnp3InactivityTimerDuration	Length of time in minutes the gateway will wait for DNP3 traffic from a SCADA master before performing recovery actions to restore DNP3 connectivity. A value of zero (0) disables the DNP3 recovery mechanism.	Integer	0 - 1500
devicename	User-specified device name, to be reported via DNP3 in group 0, attribute 247. See Gateway Name on <i>Gateway Settings</i> screen.	String	n/a
gangOperationEnabled	This setting disables the <b>Gang Operation</b> feature in the gateway, independent of the individual settings for the TripSaver II recloser. When set to "true," the <b>Gang Operation</b> feature is enabled and will operate according to the settings defined on the <b>Gang/Local</b> tab for each TripSaver II recloser. When set to "false," the <b>Gang Operation</b> feature will not operate.	Boolean	True or False
gangOperationMaxRetries	The maximum number of times the gateway will retry a gang operation after timing out in its initial attempt. Used with gangOperationRetryTime. A value of zero (0) disables the gang operation retry mechanism.	Integer	0 - 2592000
gangOperationRetryTime	The time interval between gang operation retry attempts in seconds.	Integer	1 - 3600
unsolRespDelayEventCount	The maximum number of DNP3 unsolicited events the gateway will queue before sending to the SCADA master. A value of one (1) disables the queuing mechanism so the gateway will immediately send all unsolicited events.	Integer	1 - 60
unsolRespDelayTime	The maximum amount of time the gateway will queue DNP3 unsolicited events before sending to the SCADA master, in units of milliseconds.	Integer	100 - 120000

TABLE CONTINUED ►

**Table 1. Import and Export ConfigDB Parameters—Continued**

Name	Description	Data Type of Value	Range of Value
enableSingleUnitOperation	This setting enables or disables the single-unit <b>Drop Open</b> feature in the gateway, independent of the individual settings for the TripSaver II recloser. When set to “true,” the single-unit <b>Local Drop Open</b> feature is enabled and will operate according to the settings defined on the <b>Gang/Local</b> tab for each TripSaver II recloser. When set to “false,” the <b>Single Unit Operation</b> feature will not operate.	Binary	True or False
remoteDropOpenEnabled	This setting enables or disables the <b>Remote Drop Open</b> feature in the gateway, independent of the individual settings for the TripSaver II recloser. When set to “true,” the <b>Remote Drop Open</b> feature is enabled and will operate according to the settings defined on the <b>Gang/Local</b> tab for each TripSaver II recloser. When set to “false,” the <b>Remote Drop Open</b> feature will not operate.	Binary	True or False
IECtoggle	This setting determines the SCADA protocol the gateway will use. When set to “false,” the gateway will use DNP3. When set to “true,” the gateway will use IEC 60870-5-104. For more details on IEC 60870-5-104, refer to S&C Instruction Sheet 461-519.	Boolean	True or False
timeSyncSource	This setting specifies the source(s) the gateway will use for time synchronization. When set to “gps,” the gateway will only rely on GPS for time synchronization. When set to “SCADA,” the gateway will only synchronize with the DNP3 SCADA master. When set to “gpsScada,” the gateway will rely on GPS as its highest priority time synchronization source and use DNP3 as a backup method.	String	gps, scada, gpsScada



## Configuring the Communications Gateway

The second section in the XML file format is encapsulated by <DNP3> tags. This contains more structured information such as the list of binary input setpoint mappings, for example:

```
<DNP3>
  <BinaryInputSetPoints>
    <binaryinputsetpoint statuspoint="0" codedescription="1" eventclass="2"/>
    <binaryinputsetpoint statuspoint="3" codedescription="2" eventclass="1"/>
  </BinaryInputSetPoints>
</DNP3>
```

The configuration settings that can be specified in this section of the document are described in Table 2.

**Table 2. Import and Export Settings Configuration**

Parameter Group	Attribute	Description	Data Type	Range of Value
<DNP3Masters> <dnpp3master/> </DNP3Masters>	unsolicitedenabled	Boolean indicating whether the gateway will attempt to send DNP3 unsolicited responses to the SCADA master. See Unsolicited Response on <i>DNP3 Master Settings</i> screen.	Boolean	True or False
	port	Gateway's TCP or UDP listen port for receiving IP packets from the SCADA master.	Integer	1024 ... 49,151
	ipaddress	SCADA master's IP address. Currently ignored by the gateway as it will accept traffic from any IP address. See IPv4 Address on <i>DNP3 Master Settings</i> screen.	IP address (dotted decimal)	Any valid IP address
	dnpp3address	SCADA master's DNP3 address. See DNP3 Address on <i>DNP3 Master Settings</i> screen.	Integer	1 ... 65,519
<BinaryInputSetPoints> <binaryinputsetpoint/> </BinaryInputSetPoints>	statuspoint	See Status Point on <i>DNP3 Outstation Settings</i> screen.	Integer	0 ... 147
	codedescription	See Code Description on <i>DNP3 Outstation Settings</i> screen.	Integer	Per S&C Instruction Sheet 461-560
	eventclass	See Class on <i>DNP3 Outstation Settings</i> screen A value of 0 corresponds to NO EVENT.	Integer	0,1,2,3

TABLE CONTINUED ►

Table 2. Import and Export Settings Configuration—Continued

Parameter Group	Attribute	Description	Data Type	Range of Value
<AnalogInputSetPoints> <analoginputsetpoint/> </AnalogInputSetPoints>	statuspoint	See Status Point on <i>DNP3 Outstation Settings</i> screen.	Integer	0...20
	codedescription	See Code Description on <i>DNP3 Outstation Settings</i> screen.	Integer	Per S&C Instruction Sheet 461-560
	eventclass	See Class on <i>DNP3 Outstation Settings</i> screen. A value of 0 corresponds to NO EVENT.	Integer	0,1,2,3
	fixeddeadband	See Fixed Deadband on <i>DNP3 Outstation Settings</i> screen. Set to 'disabled' to disable fixed deadband reporting for this setpoint.	Integer or "disabled"	Any non-negative integer value or "disabled"
	percentdeadband	See Pct Deadband on <i>DNP3 Outstation Settings</i> screen. Set to "disabled" to disable percent deadband reporting for this setpoint.	Integer or "disabled"	Any non-negative integer value or "disabled"
	scaling	Floating point scaling factor, to be applied as a multiplication factor to the raw setpoint measurement before it is sent to the SCADA master. See Scaling on <i>DNP3 Outstation Settings</i> screen.	float	0.001 ... 1000
<CounterSetPoints> <countersetpoint/> </CounterSetPoints>	statuspoint	See Status Point on <i>DNP3 Outstation Settings</i> screen.	Integer	0 ... 19
	codedescription	See Code Description on <i>DNP3 Outstation Settings</i> screen.	Integer	Per S&C Instruction Sheet 461-560
	eventclass	See Class on <i>DNP3 Outstation Settings</i> screen. A value of 0 corresponds to NO EVENT.	Integer	0,1,2,3
	fixeddeadband	See Fixed Deadband on <i>DNP3 Outstation Settings</i> screen. Set to "disabled" to disable fixed deadband reporting for this setpoint.	Integer or "disabled"	Any non-negative integer value or "disabled"
	percentdeadband	See Pct Deadband on <i>DNP3 Outstation Settings</i> screen. Set to "disabled" to disable percent deadband reporting for this setpoint.	Integer or "disabled"	Any non-negative integer value or "disabled"
<BinaryOutputSetPoints> <binaryoutputsetpoint/> </BinaryOutputSetPoints>	statuspoint	See Status Point on <i>DNP3 Outstation Settings</i> screen.	Integer	0 ... 8
	codedescription	See Code Description on <i>DNP3 Outstation Settings</i> screen.	Integer	Per S&C Instruction Sheet 461-560
	Retry Behavior	Will either discard the retry attempt or retry for the set interval and number of attempts.	Binary	Discard or Queue
	Retry Interval	Time, in seconds, between retry attempts.	Integer	1 to 3600
	Max Retry Attempts	The maximum number of times the output will be retried.	Integer	1 to 2,592,000

# Configuring the Communications Gateway

## Import Configuration

Follow these steps to complete the **Import Configuration** function. See Figures 22 and 23.

- STEP 1.** Under the Gateway Configuration panel, click on the **Import Configuration** button. A Web User Interface (WUI) dialog box appears.
- STEP 2.** Click on the **Browse** button, which invokes a Windows file navigation box.
- STEP 3.** Navigate to the file.
- STEP 4.** Highlight the file and click on the **Open** button. The highlighted file will then be identified in the WUI dialog box.
- STEP 5.** Click on the **Import** button.
- STEP 6.** Click on the **Save** button.

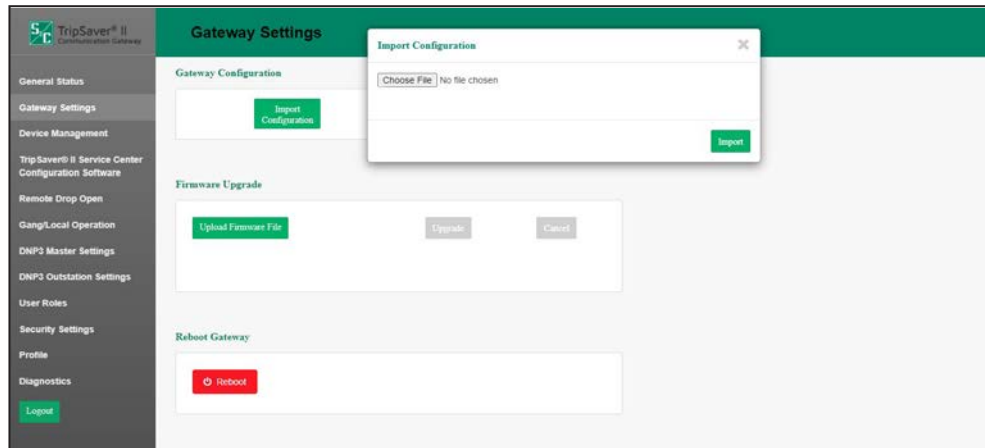


Figure 22. The Import Configuration dialog box.

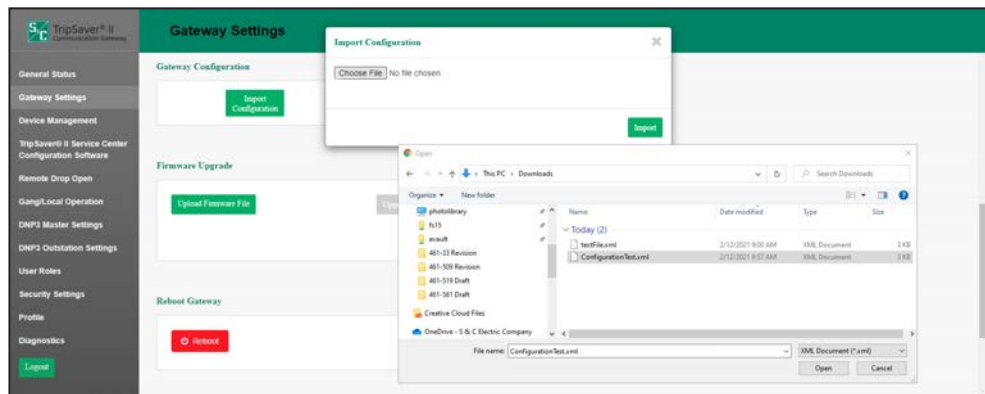


Figure 23. Import file navigation.

## Export Configuration

Follow these steps to complete the **Export Configuration** function. See Figures 24 and 25.

- STEP 1.** On the Gateway Configuration panel, click on the **Export Configuration** button. A WUI dialog box appears with a suggested filename for the exported configuration. The default name is textFile but can be changed.
- STEP 2.** Click on the **Export** button.
- STEP 3.** Wait a few seconds for the exported file to appear in your browser. The file will be stored in the Downloads folder.

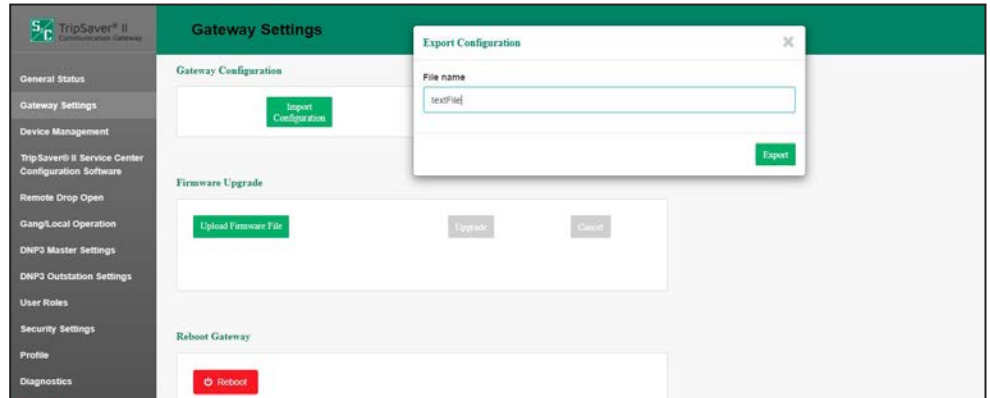


Figure 24. The Export Configuration dialog box.

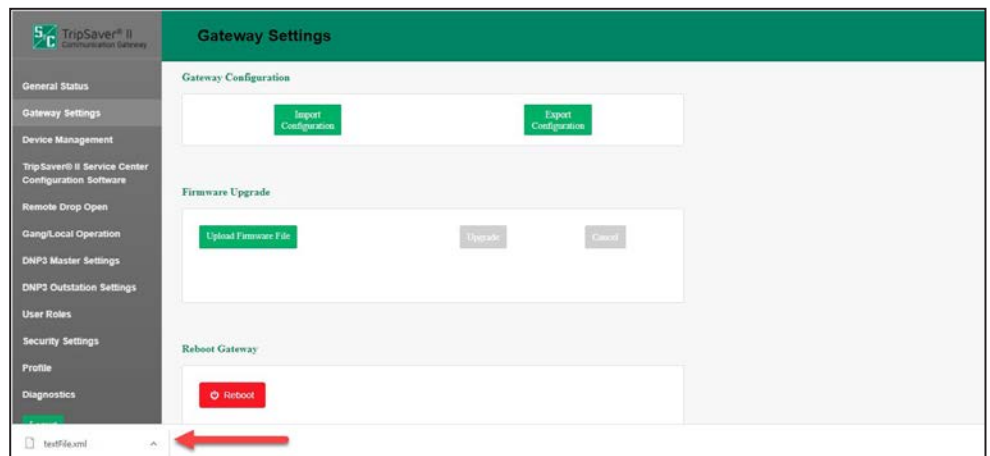


Figure 25. Export File Save navigation.

## Firmware Upgrade

This panel enables the loading of firmware versions onto the communications gateway. See Figure 26.

Follow these steps to perform a firmware upgrade:

**STEP 1.** Download the firmware file. Firmware files can be found in the S&C Customer Portal at [sandc.com/en/support/sc-customer-portal/](http://sandc.com/en/support/sc-customer-portal/).

**STEP 2.** Click on the **Upload Firmware File** button on the Firmware Upgrade panel. See Figure 26.

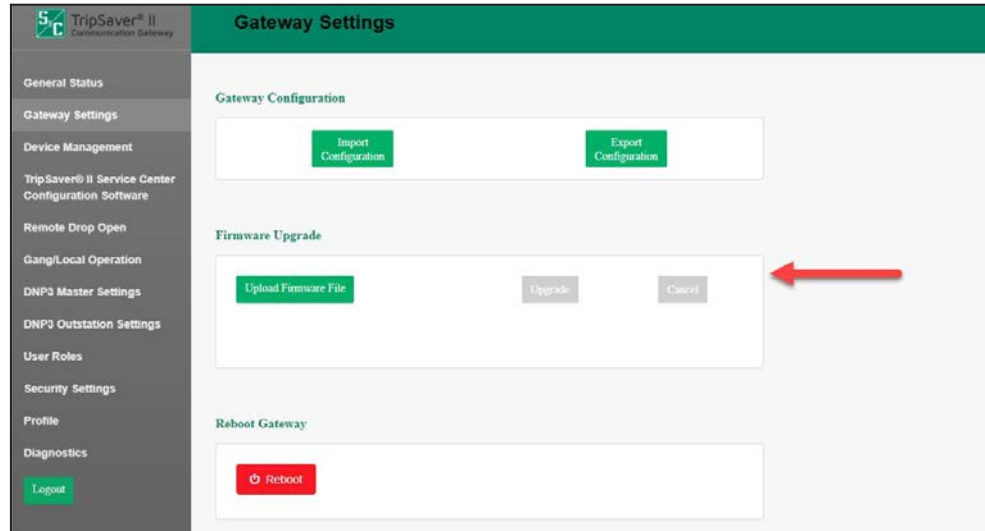
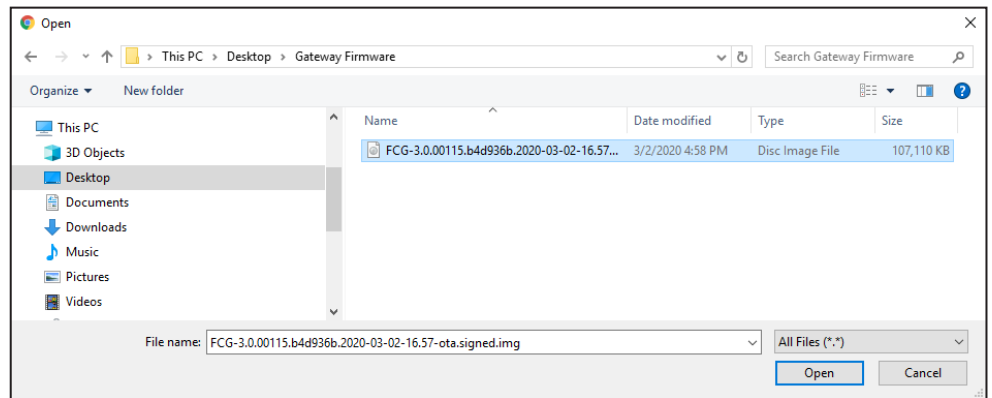


Figure 26. The Firmware Upgrade panel.

**STEP 3.** A Windows dialog box will open. See Figure 27. Navigate to the firmware file and select it. Click on the **Open** button.



**Figure 27.** The firmware-upload dialog box.

# Configuring the Communications Gateway

**STEP 4.** The file uploads to the communications gateway. After the upload completes, the gateway will confirm a successful upload. See Figures 28 and 29.

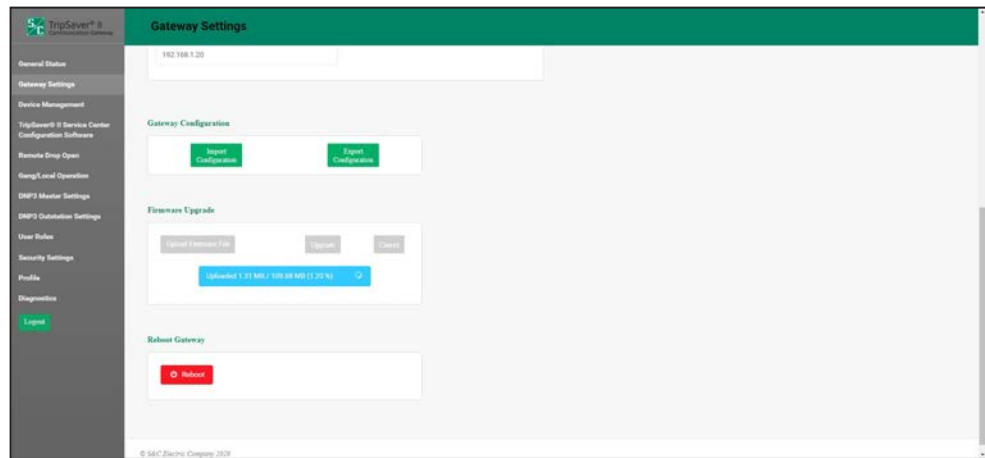


Figure 28. The Firmware Upload progress bar.

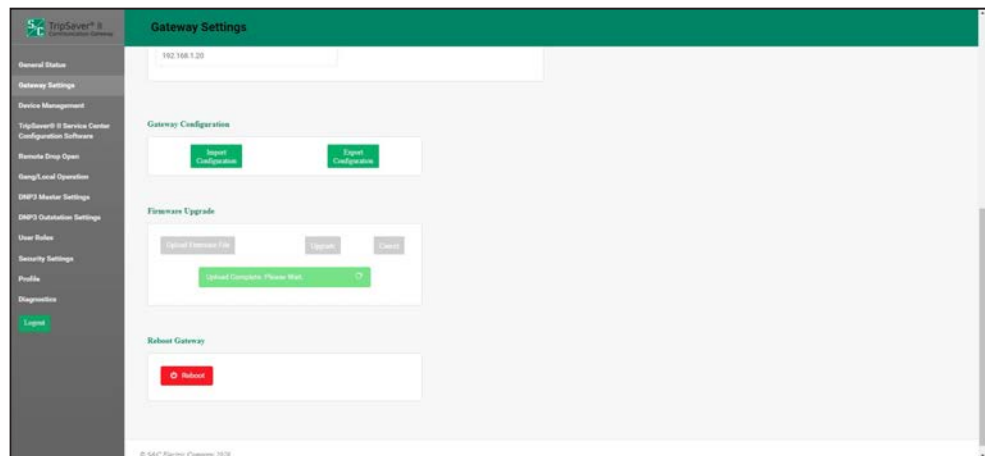
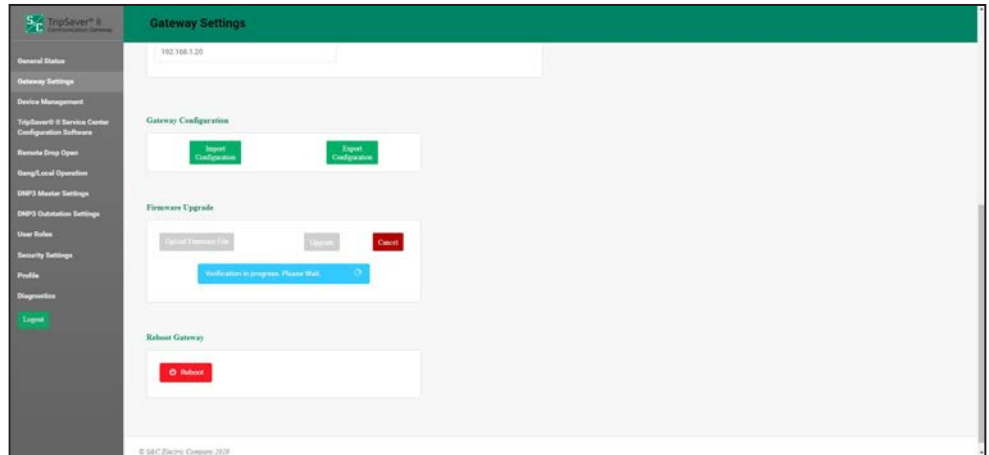


Figure 29. The dialog box showing the firmware upload is complete.

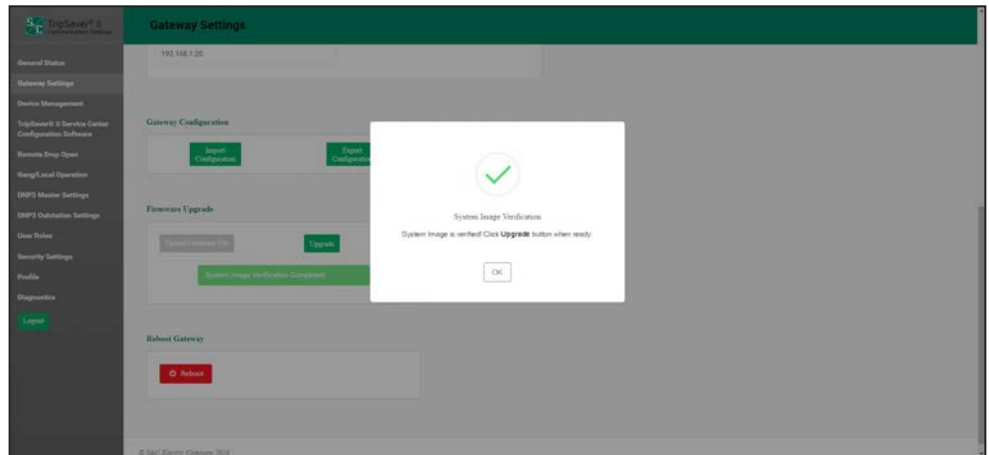


**STEP 5.** When it is 100% done, the communications gateway will go through a verification process to confirm it was securely signed by S&C Electric Company. See Figure 30.



**Figure 30.** The firmware-verification process.

**STEP 6.** After the file is verified, a notification will appear. Click on the **OK** button to dismiss this window. The **Upgrade** button will become active. See Figure 31.



**Figure 31.** The dialog box showing the firmware-verification process is complete.

# Configuring the Communications Gateway

**STEP 7.** Click on the **Upgrade** button. This will start the upgrade process. See Figures 32 and 33.

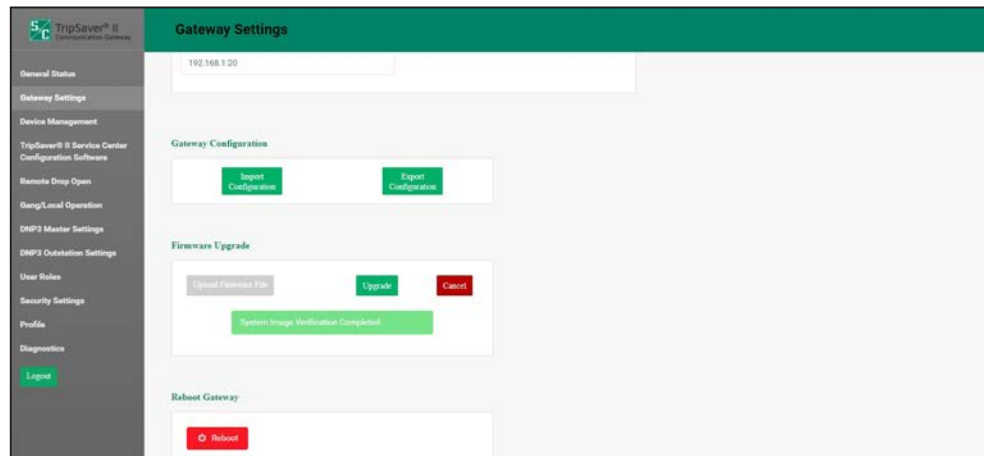


Figure 32. Start the firmware upgrade process by clicking on the Upgrade button.

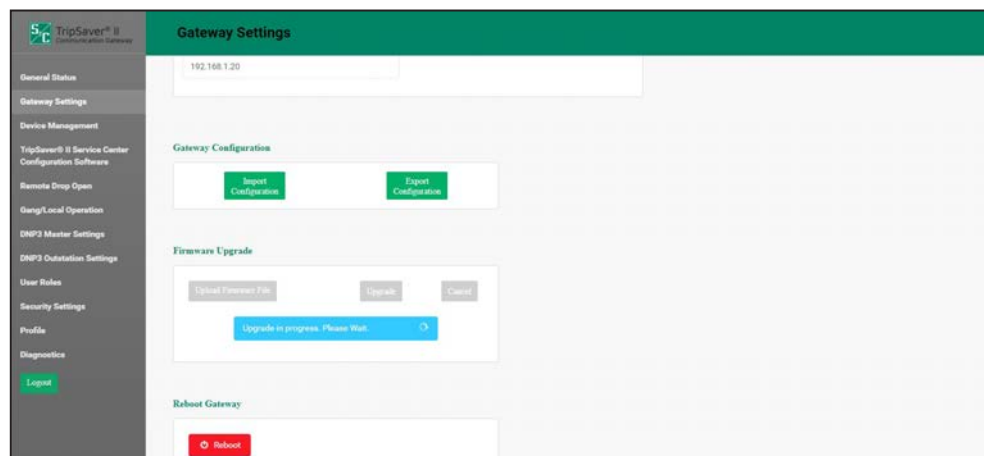


Figure 33. The firmware-upgrade process progress bar.

**STEP 8.** When the gateway has completed processing the upgrade, a notification will appear. See Figure 34. When the user clicks on the **OK** button on this notification, the browser will display a screen indicating the gateway is unavailable while it reboots. The gateway will take approximately 5 minutes to reboot. The user interface will automatically load the *Login* screen after the reboot completes. See Figure 11 on page 21. Log in and confirm the new firmware has been installed successfully by going to the *General Status* screen.

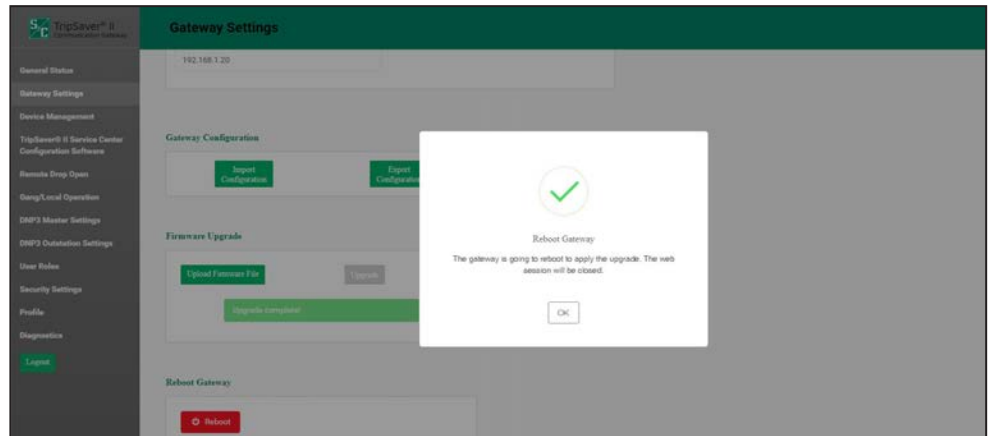


Figure 34. The dialog box showing the firmware upgrade is complete.

## Reboot Gateway

The red **Reboot** button enables the user to restart the communications gateway. See Figure 35. When selected, a dialog box appears to confirm the **Reboot** command. After the user clicks on the **OK** button, the user interface will show a *Gateway Unavailable* screen. The entire reboot process requires approximately 5 minutes before communications to the communications gateway are re-established. When the reboot is complete, the user interface will automatically load the *Login* screen. See Figure 11 on page 21.

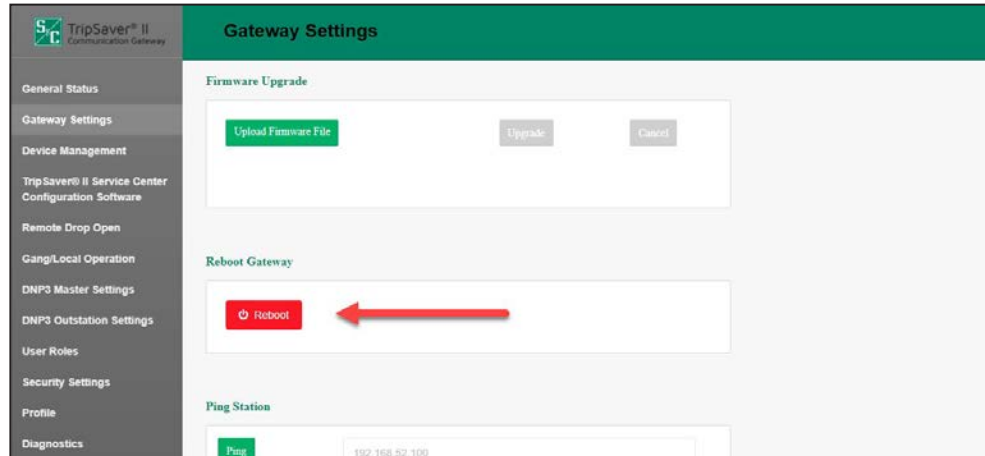


Figure 35. The Reboot Gateway button.

## Ping Station

The **Ping Station** feature allows the user to ping the SCADA master station or any connected IP address. This feature allows the user to confirm the gateway is correctly connected to the user's network. Type in the IP address of the SCADA master station or other device, and click on the **Ping** button. See Figure 36 and Figure 37 on page 45. A Success message will appear, and the results of the ping will display as text in the Ping Station panel. If the ping is unsuccessful, a Results message will appear in the panel showing what went wrong.

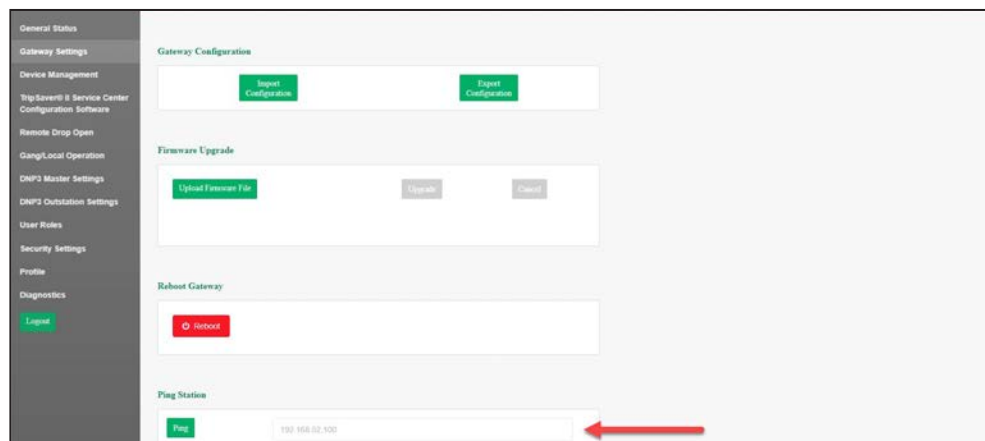
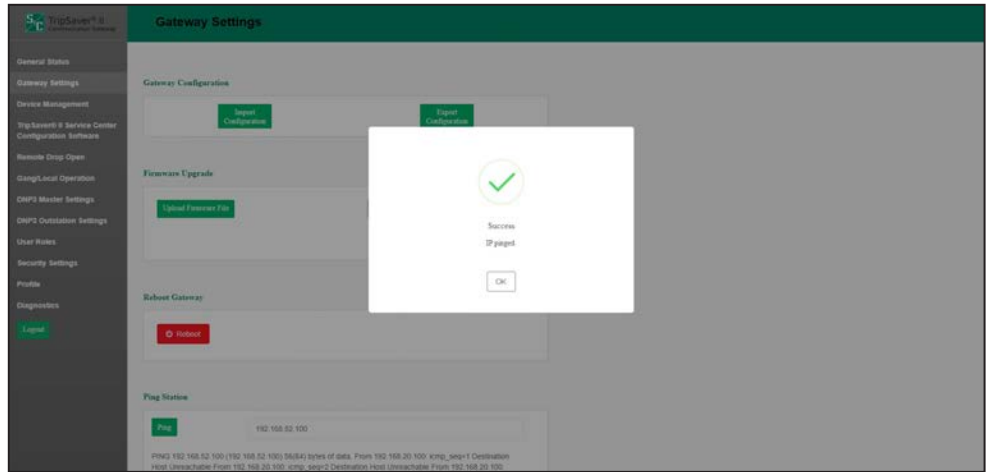


Figure 36. Location of the Ping Station button.



**Figure 37. A ping Success message.**

## Device Management

The purpose of the *Device Management* screen is to provide the ability to add, modify, update, or delete a TripSaver II recloser. Additionally, a listing of TripSaver II reclosers with respective connection status is displayed in the screen. See Figure 38 on page 46.

**Note:** To pair a TripSaver II recloser with the communications gateway, the recloser must be in **Gateway** mode. **Gateway** mode is set using the service center configuration software and the service center configuration kit (USB transceiver and power module). Refer to S&C Instruction Sheet 461-504, “TripSaver® II Cutout-Mounted Recloser: *Protection Setup Using Service Center Configuration Kit*,” for complete instructions on connecting to a TripSaver II recloser with the USB transceiver and power module and enabling **Gateway** mode.

### NOTICE

The unpairing or deleting of a TripSaver II recloser(s) from the communications gateway will remove the recloser’s wireless communications capability. To re-enable wireless (**Gateway** mode), the TripSaver II recloser(s) must be removed from the pole and accessed via the TripSaver II Service Center Configuration Software, USB transceiver, and corded power module. Refer to S&C Instruction Sheet 461-504, “TripSaver® II Cutout-Mounted Recloser: *Protection Setup Using Service Center Configuration Kit*,” for complete instructions on connecting to a TripSaver II recloser with the USB transceiver, corded power module, and ac adapter. See the “Commissioning (Pairing) a TripSaver II Recloser for Use with the Communications Gateway” section on page 78 for a description of the pairing process.

## Configuring the Communications Gateway

To add a TripSaver II recloser, click on the **Add TripSaver II** button on the top right of the page. A dialog box will appear. Enter the recloser's Transceiver ID and the desired device name. See Figure 38 and Figure 39. The Transceiver ID must contain a total of 32 hexadecimal digits, separated by three periods. After the process is completed, the user will be returned to the top of the TripSaver II Device Management panel when the **Add** button is clicked. For full instructions on pairing a TripSaver II recloser with the communications gateway, see the "Commissioning (Pairing) a TripSaver II Recloser for Use with a Communications Gateway" section on page 78.

**Note:** The **TripSaver II Device Name** field is optional and may be left blank.

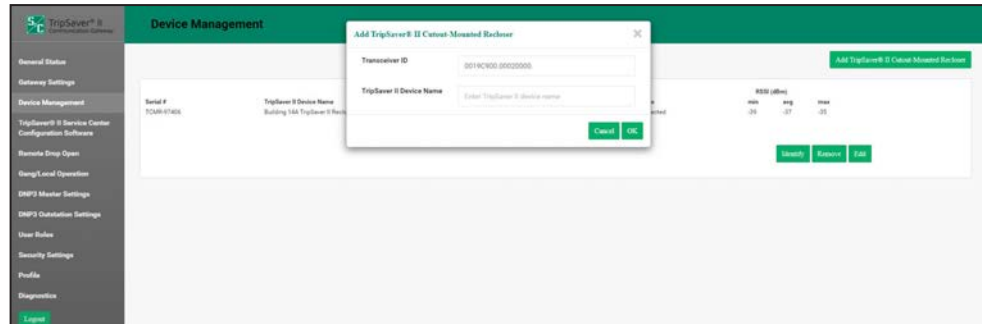


Figure 38. Pairing of a TripSaver II recloser with the communications gateway.

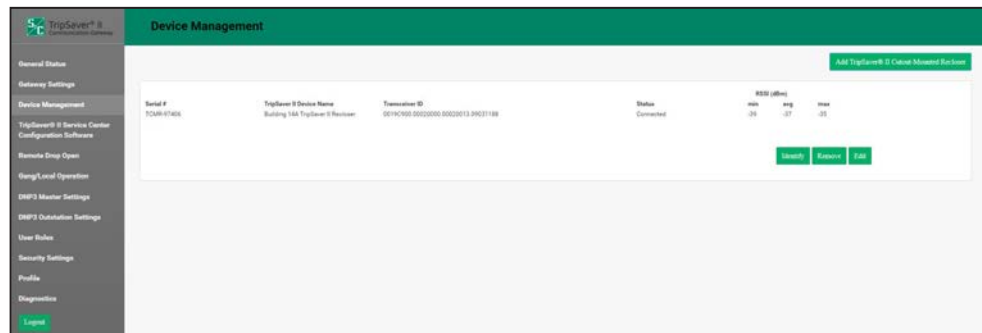


Figure 39. The screen showing the successful addition of a TripSaver II recloser and status.

The top *TripSaver II Device Management* screen will display on a single line the added recloser and any other TripSaver II reclosers that have their radios associated with this communications gateway. In addition to the serial number and TripSaver II recloser name, the recloser's Transceiver ID, link status, and RSSI are displayed.

A TripSaver II recloser may be changed or removed by clicking on the **Edit** or **Remove** button. Clicking on the **Identify** button will cause the TripSaver II recloser to update its LCD screen to all blue, then all white, and repeat. This can help to identify a specific TripSaver II recloser.

## TripSaver® II Service Center Configuration Software

When connected to the communications gateway through Ethernet Port 1, the connected TripSaver II reclosers can be accessed through the communications gateway with the service center configuration software. This allows the gateway to take the place of the USB transceiver. In this panel, users may enable or disable service center configuration access while connected to the communications gateway's Ethernet Port 1. Refer to Instruction Sheet 461-504 for more information about operation of the service center configuration software.

**Note:** The service center configuration software must be on the same computer that is connected to the Gateway via Ethernet Port 1.

### NOTICE

S&C recommends against making settings changes to the TripSaver II recloser when connected to the service center configuration software via the communications gateway. To make settings changes, remove the TripSaver II recloser from the utility pole and connect to it using the USB transceiver and corded power module.

To enable connection to the service center configuration software, click on the **Enable Service Center Configuration** toggle button to set the **On** position. See Figure 40.

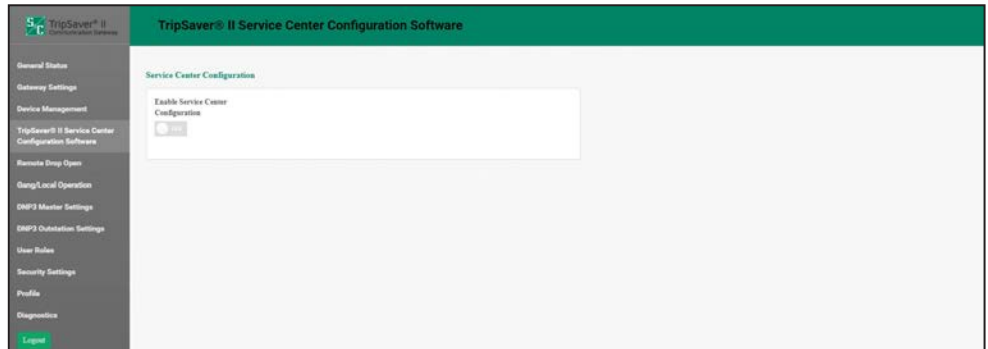
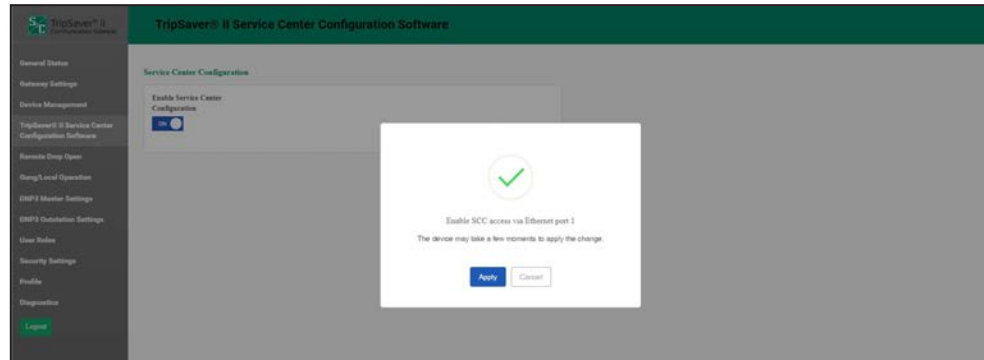


Figure 40. The Enable Service Center Configuration toggle button.



# Configuring the Communications Gateway

When the **Service Center Configuration** mode is enabled, a dialog box appears. See Figure 41.

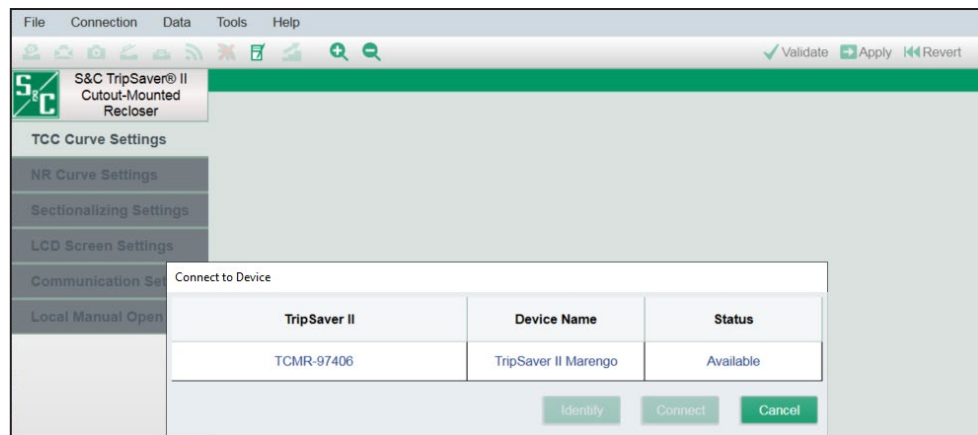


**Figure 41.** The dialog box showing the enable service center configuration pop-up.

When the service center configuration software is opened and the **Connect to Device** option is selected from the menu bar, a selection of TripSaver II reclosers connected to the gateway will be displayed. Select the desired recloser and click on the **Connect** button. The **Identify** button can be used to help identify a TripSaver II recloser. It will cycle the recloser's LCD screen to solid blue, and then back again. See Figure 42.

**NOTICE**

When using a communications gateway to connect to a TripSaver II recloser via the service center configuration software, any configuration changes made to the communications gateway during the service center configuration software session will not be captured. The communications gateway will act as a simple router directing the radio connection to the TripSaver II recloser. S&C recommends not making any changes to the communications gateway when using it to connect to a TripSaver II recloser via the service center configuration software.



**Figure 42.** The service center configuration software **Connect to Device** screen.

## Remote Drop Open

TripSaver II reclosers supplied with the **30-second** option (“-O”), firmware version 1.8 or later, and ordered with the **Remote Drop Open** option (“-D”) factory-enabled can be configured using the **Remote Drop Open** settings to operate when issued a **DNP3 SCADA** command. To use the **Remote Drop Open** feature, the TripSaver II recloser must be properly commissioned and configured with the gateway, and a SCADA transceiver must also be properly connected to the communications gateway. See the “DNP3 Outstation Settings” section on page 58 for directions on configuring the gateway with a DNP3 outstation.

The settings on the *Remote Drop Open Settings* screen only configure the feature in the communications gateway and in any properly configured TripSaver II reclosers. To receive the command, the appropriate DNP3 points must also be set. For a full list of the DNP3 points available, refer to S&C Instruction Sheet 461-560, “TripSaver® II Communications Gateway, Outdoor Distribution (15 kV and 25 kV): *DNP Points List and Implementation.*”

Each TripSaver II recloser paired with the communications gateway will appear in the device listing.

**Note:** Though the reclosers aren’t numbered in the device listing, the recloser on top is “TripSaver II recloser #1,” continuing with “TripSaver II recloser #2,” “TripSaver II recloser #3,” etc. Document this information along with the device names for later use when setting DNP3 points.

If a recloser has the **Remote Drop Open** feature (-D option) factory-enabled, the green **Factory-Enabled in TSII** indicator will display “Yes.” See Figure 43.

The **Remote Drop Open** feature is enabled in the communications gateway by toggling the **Enable Remote Drop Open in Gateway** toggle button to the **On** position. Click on the **Save** button to save settings.

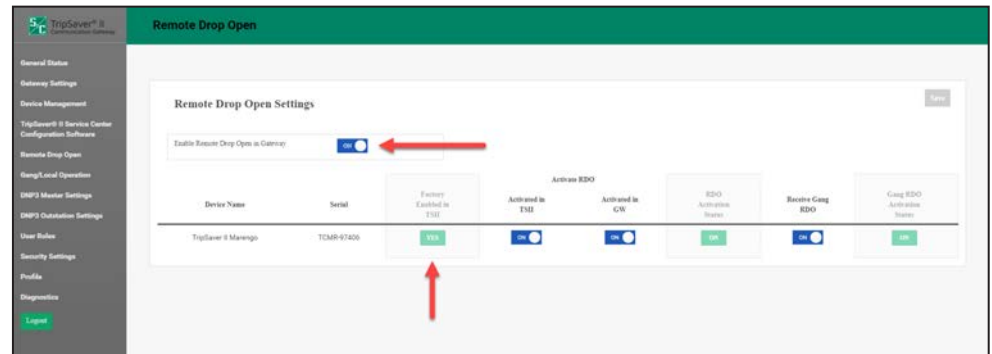
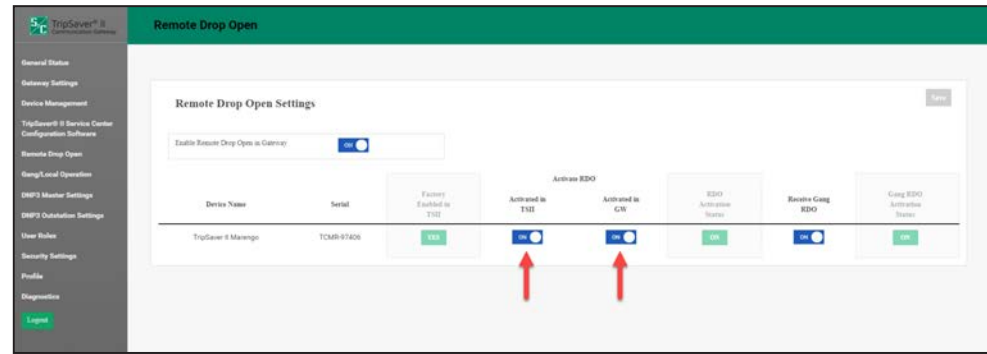


Figure 43. Enabling the Remote Drop Open feature in the communications gateway.

## Configuring the Communications Gateway

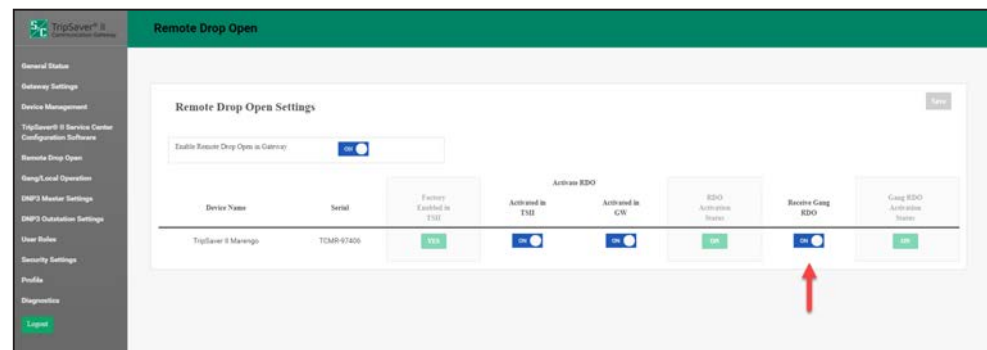
**Note:** The **Enable Remote Drop Open in Gateway** toggle button will not erase the settings for each individual recloser when toggled to the **Off** position and then saved by clicking the **Save** button. It will turn the feature off in the communications gateway. This allows the user to locally turn remote operation off if, for example, local work is to be done on a recloser group and then turn the feature back on without losing settings.

After the **Remote Drop Open** feature is activated in the TripSaver II recloser and in the communications gateway by toggling the **Activated in TSII** and **Activated in GW** toggle buttons to the **On** position, click on the **Save** button to save the settings. See Figure 44.



**Figure 44. Activating the Remote Drop Open feature in the TripSaver II recloser and the communications gateway.**

To allow the recloser to gang-operate because of a **Gang Remote** command, toggle the **Receive Gang RDO** toggle button to the **On** position. Click on the **Save** button to save the settings. Up to four reclosers can be configured to remotely gang-operate in response to a **DNP3 Communications Gateway Remote Gang Drop Open** command. See Figure 45.



**Figure 45. Enabling Remote Receive Gang operation for the TripSaver II recloser.**

When a TripSaver II recloser that does not have the **Remote Drop Open** option (“-D”) factory-enabled is paired with the communications gateway, the **Factory Enabled in TSII** setting will show a grey “NO” label, and the two **Activation Status** indicators will also show a grey “NO” label. See Figure 46.

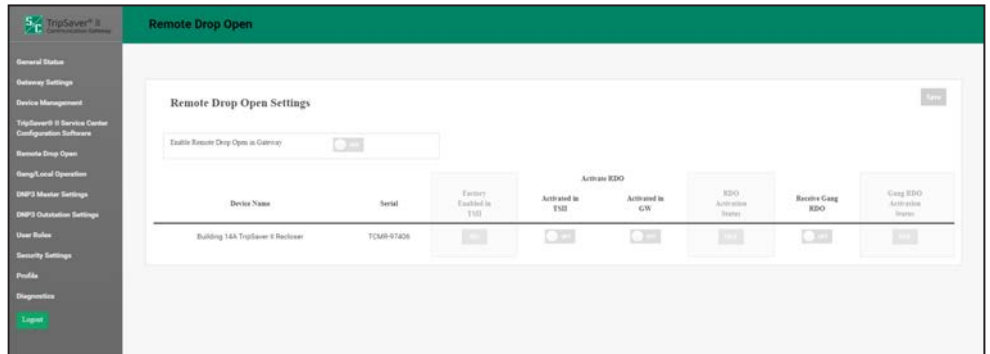
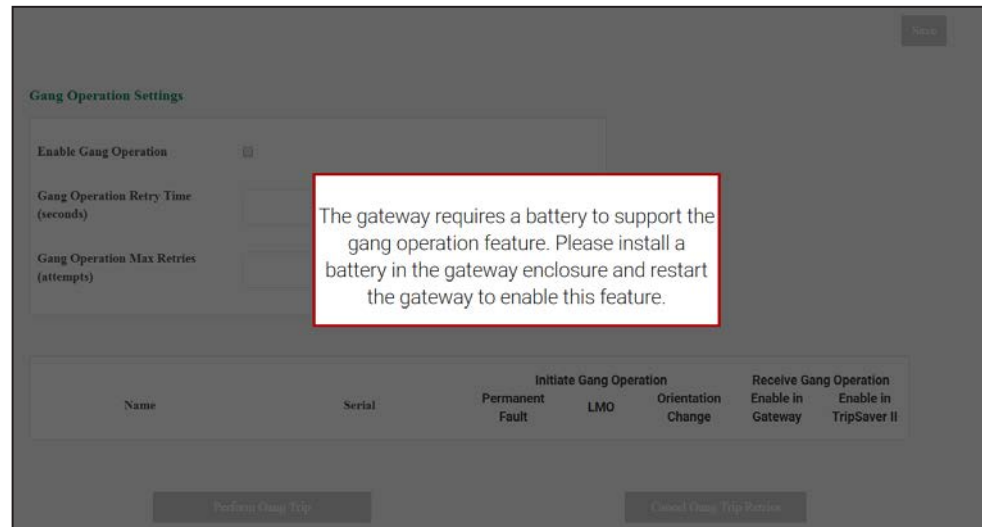


Figure 46. A TripSaver II recloser when the Remote Drop Open feature is not factory-enabled in the recloser.

## Gang/Local Operation

### Local Drop Open Operation Settings

TripSaver II reclosers supplied with firmware versions 1.7 and later can be configured using the **Local Drop Open** settings to drop open when another member of the configuration group, or “gang,” drops open because of a permanent fault, **Local Manual Open** (LMO) operation, or an orientation change. (These operations are overseen directly by the gateway and are not signaled by a SCADA master station via DNP3.) This feature is called **Gang Operation**. If no backup battery is available in the communications gateway enclosure, this screen will be disabled. See Figure 47.

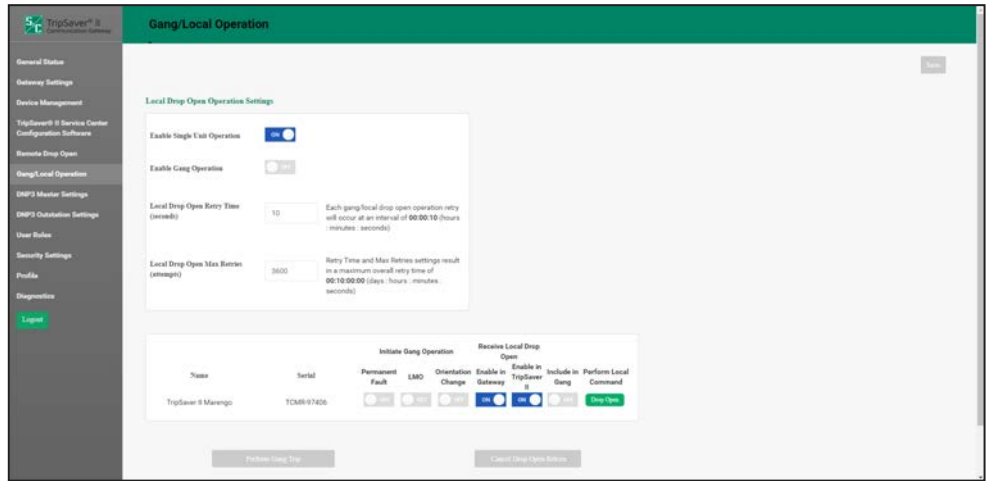


**Figure 47. The communications gateway requires a backup battery for Local/Gang operation.**

New to TripSaver II Communications Gateway firmware versions 3.0 and 4.0 and only available with TripSaver II recloser firmware versions 1.8 or later is the ability to allow a **Local Single Unit** drop-open function of TripSaver II reclosers paired with a communications gateway.

The **Enable Single Unit Operation** button, when toggled on, allows a user logged in to the gateway to perform a **Local Drop Open** command for a single unit paired with the gateway by clicking the green **Drop Open** button in the “Perform Local Command” column. This single-unit operation feature works regardless of whether the TripSaver II

recloser is configured to work in a gang. For this feature to work, the **Receive Local Drop Open** setting must be enabled in both the gateway and the TripSaver II recloser by toggling the appropriate buttons to the **On** position. Click on the **Save** button after making the desired settings. See Figure 48.



**Figure 48. Enabling the single-unit Local Drop Open operation.**

The **Gang Operation** feature is enabled by toggling the **Enable Gang Operation** button to the **On** position.

To be a member of a gang operation group, the TripSaver II must have the **Receive Local Drop Open** feature enabled in both the communications gateway and the TripSaver II recloser by toggling both the **Enable in Gateway** and **Enable in TripSaver II** buttons to the **On** position as well as having the **Include in Gang** button toggled to the **On** position. Click on the **Save** button after making the desired settings.

The **Enable in Gateway** toggle button must be set to allow the gateway to gang operate the TripSaver II recloser, while **Enable in TripSaver II** toggle button enables the same drop-open capability in the TripSaver II recloser itself. The **Enable in TripSaver II** setting can also be modified via SCADA using a DNP3 command or with the TripSaver II Service Center Configuration Software. Both the **Enable in Gateway** and **Enable in TripSaver II** toggle buttons must be toggled to the **On** position for a TripSaver II recloser to drop open because of a gang operation or by using the green **Drop Open** button under the “Perform Local Command” column.

# Configuring the Communications Gateway

To enable a TripSaver II recloser to be an initiator of a gang operation, one or more of the **Initiate Gang Operation** toggle buttons must be toggled to the **On** position. The three initiator buttons are **Permanent Fault**, **Local Manual Open (LMO)**, or **Orientation Change**. See Figure 49.

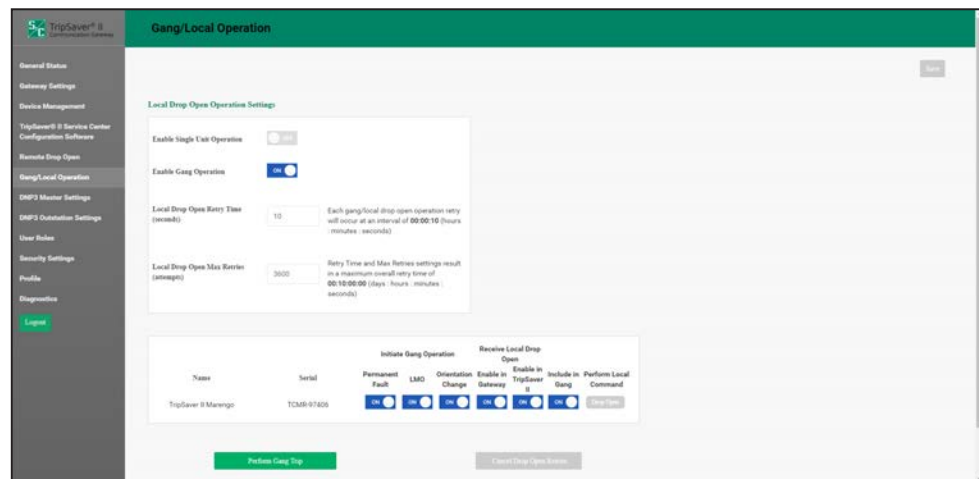


Figure 49. Enabling a Gang operation.

Two other features that should be configured are the **Local Drop Open Retry Time** and the **Local Drop Open Max Retries**. See Figure 50.

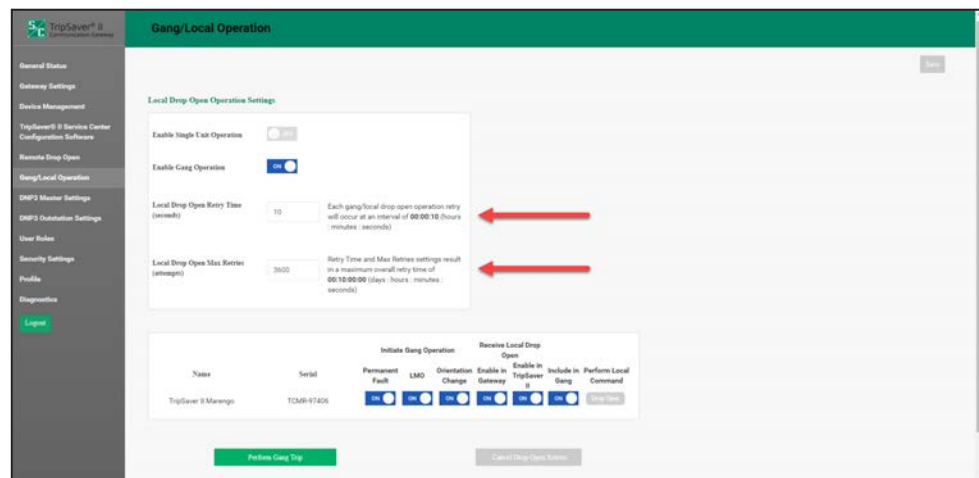


Figure 50. Configuring the Retry Time and Maximum Number of Retries settings.



The **Local Drop Open Retry Time** (seconds) field configures the time between drop-open commands given to the reclosers, either directly by clicking the **Perform Local Command** button or when configured for gang operation. (Range: 0-3600 seconds; Default: 10)

The **Local Drop Open Max Retries** field configures the maximum number of **Gang/Local** operation commands to be given to the reclosers configured for **Gang/Local** operation. (Range: 0-2,592,000)

After making the desired settings, click on the **Save** button to save the configuration.

The **Perform Gang Trip** button can be clicked to perform a local **Gang Operation** function on user request. When this button is clicked, the user will be asked to provide a walkaway time interval, in seconds. After this time interval, the gateway will perform the **Gang Trip** operation.

**⚠ WARNING**

Enter a walkaway time long enough to give any personnel underneath the TripSaver II reclosers enough time to walk away. Do not stand underneath the TripSaver II reclosers during a gang operation. Failure to walk away could result in severe personal injury.

The **Cancel Drop Open Retries** button will be enabled when a **Gang Operation** procedure is active and performing periodic retries. When this button is clicked, the communications gateway will immediately halt the retries and will abandon the **Drop Open** operation. See Figure 51.

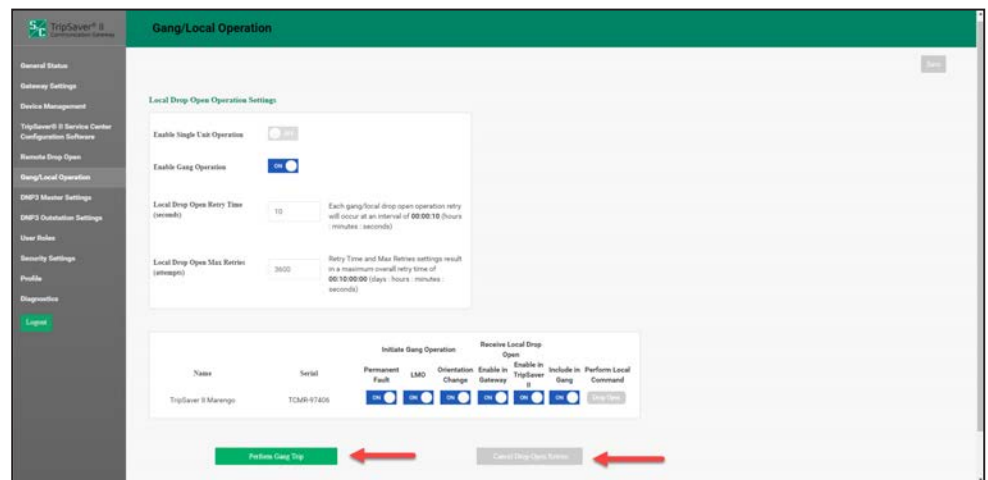


Figure 51. Performing a Gang Trip operation.

# Configuring the Communications Gateway

A TripSaver II recloser and paired communications gateway can be configured for both **Single Unit Operation** and **Gang Operation** functions. See Figure 52.

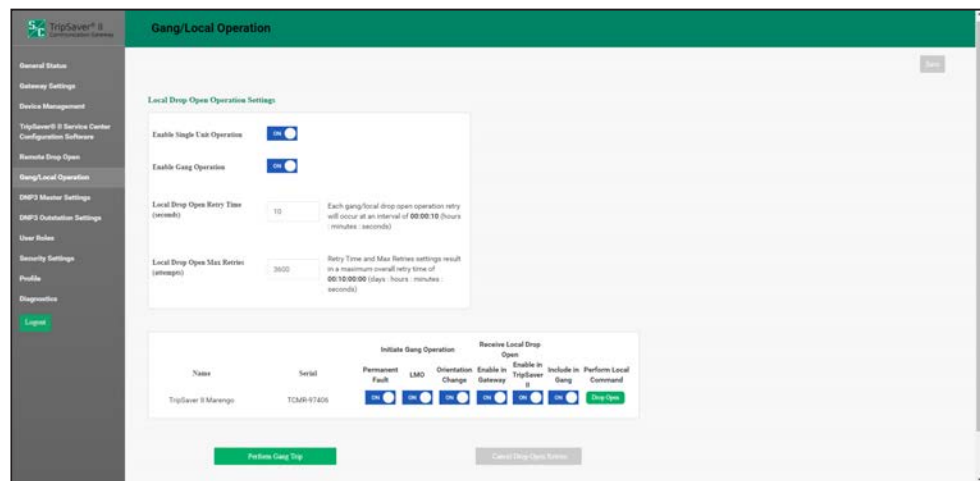


Figure 52. A Single Unit and Gang operation.

## DNP3 Master Settings

The purpose of the *DNP3 Master Settings* screen is to update settings for connecting to the DNP3 master server.

### General DNP3 Master Settings

The backhaul communications protocol is first identified by the selection of **TCP**, **UDP**, or **Serial** options in the drop-down box. When chosen, the **Save** button must be clicked. See Figure 53.

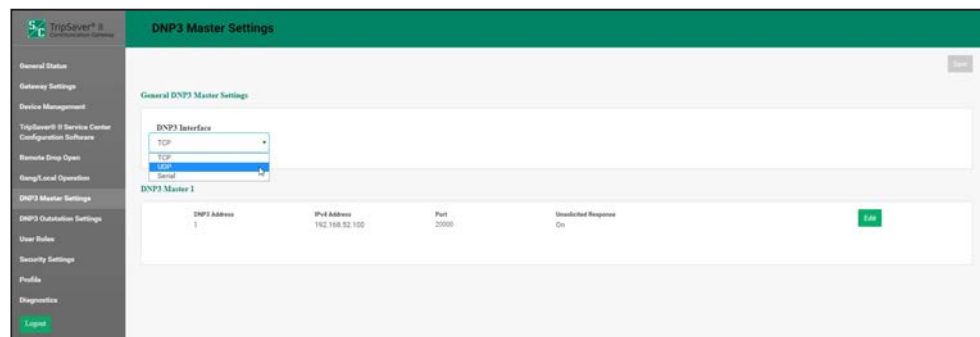


Figure 53. The DNP3 master protocol interface drop-down box.

Specific to the selection of the serial protocol, four new fields will open directly under the General DNP3 Master Settings panel. The new fields requiring input include **Baud Rate**, **Stop Bits**, **Parity**, and **Flow Control**. The **Baud Rate** field is chosen by selecting one of the values from the drop-down menu. The **Stop Bits**, **Parity**, and **Flow Control** fields are radio buttons that require selection. (**Data Bits** is always set to 8, and it cannot be changed.) Finally, click on the **Save** button to finalize the field edits. See Figure 54.

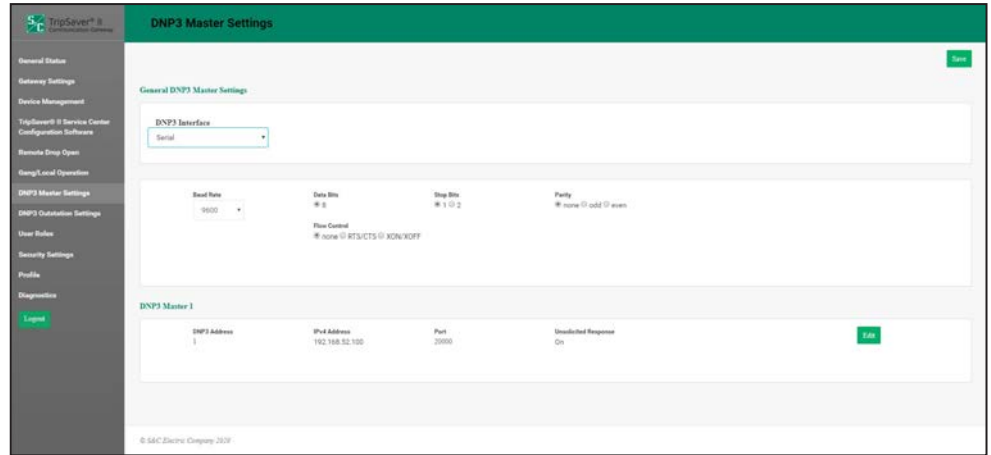


Figure 54. The DNP3 Master with serial configuration panel.

## DNP3 Master 1

The DNP3 Master 1 panel allows updates to the **DNP3 Address**, **IPv4 Address**, **Port**, and **Unsolicited Response** fields. After clicking on the **Edit** button, a dialog box appears for specific field inputs. The DNP3 address must be specified regardless of the selection of TCP, UDP, or Serial transport. The **Unsolicited Response** field is set to the **On** position. The port value is used as the gateway's local listen port when either TCP or UDP transport is selected. Finally, the **IP address** field is presently ignored. When either TCP or UDP transport is selected, the gateway will accept traffic from any IP address and will send responses to that same IP address. Click on the **Save** button to save the modifications. See Figure 55.

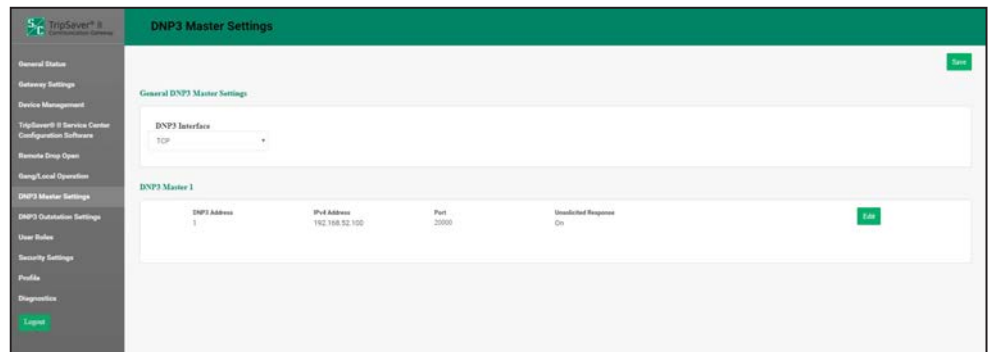


Figure 55. The DNP3 Master with serial configuration panel.

## DNP3 Outstation Settings

The purpose of the *DNP3 Outstation Settings* screen is to specify how the communications gateway will operate within a **Proxy** mode between the TripSaver II recloser and the SCADA master and to configure the DNP3 point codes/mapping for DNP3 communications to the TripSaver II recloser. In this firmware release, version 4.0, the communications gateway will operate in **Concentrator** mode only. **RTU Concentrator** mode (default) hosts a single RTU DNP3 address for all TripSaver II reclosers it supports. The communications gateway will deliver information for each TripSaver II recloser mapped to separate point codes, providing more efficient SCADA integrity poll messaging overhead and conserving DNP address space.

**Note:** The Web-user interface enforces a 30-minute session inactivity timer. When many inputs are required, it is recommended to routinely save settings.

### DNP3 Addressing

In this panel, the addressing type is fixed as **Concentrator** mode, while the **Gateway DNP3 Address** field may be edited. For the **Gateway DNP3 Address** field, enter the DNP3 address identified on the SCADA master to the corresponding communications gateway. See Figure 56.

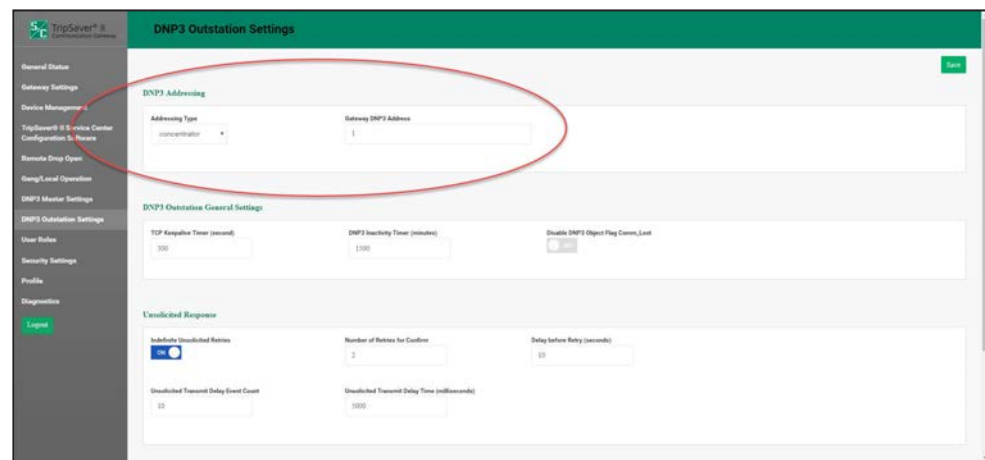


Figure 56. The DNP3 Addressing panel.

## DNP3 Outstation General Settings

In this panel are two fields and one toggle button, the **TCP Keepalive Timer** and the **DNP3 Inactivity Timer** fields and the **Disable DNP3 Object Flag Comm Lost** toggle button, specific to settings for communications between the communications gateway and the SCADA master. See Figure 57.

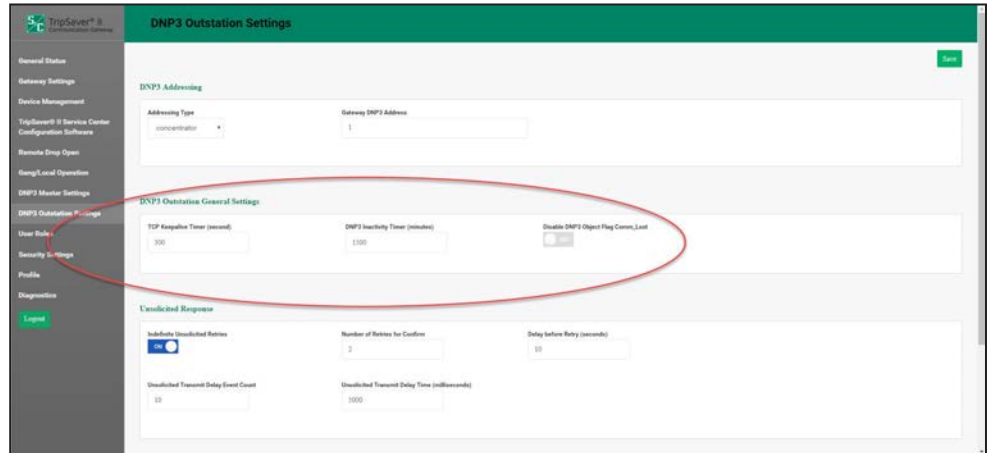


Figure 57. The DNP3 Outstation General Settings panel.

The fields are defined as follows:

- **TCP Keepalive Timer.** This field is a heartbeat timer and is the interval between the DNP3 keepalive messages sent over a TCP connection.
- **DNP3 Inactivity Timer.** This is the length of time, in minutes, the gateway will wait for DNP3 traffic from a SCADA master before performing recovery actions to restore DNP3 connectivity. A value of zero (0) disables the DNP3 recovery mechanism.
- **Disable DNP3 Object Flag Comm\_Lost.** This setting disables the Comm\_Lost flag in DNP3 standard object flags. When enabled, the Comm\_Lost flag can cause frequent DNP3 events.

### Unsolicited Response

The DNP3 unsolicited response capability allows the communications gateway to report event data to the SCADA master in real time without waiting for a request from the master. See Figure 58.

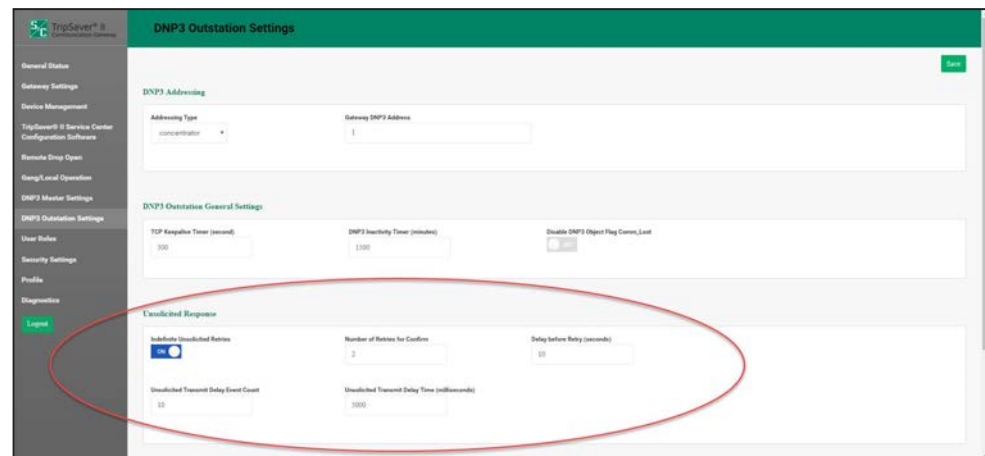


Figure 58. The Unsolicited Response panel.

The fields are defined as follows:

- **Indefinite Unsolicited Retries.** This toggle button enables the communications gateway to keep retrying the transmittal of cached TripSaver II recloser unsolicited responses until successful back to the SCADA master.
- **Number of Retries for Confirm.** This field is only relevant when the **Unsolicited Responses Retried Indefinitely** function is disabled. In this case, the field defines the maximum number of transmittal retries for an unsolicited response messages back to the SCADA master(s).
- **Delay Before Retry.** This represents the delay before the first retry of a queued TripSaver II recloser unsolicited response. Subsequent retries will be sent after increasing amounts of delay to minimize network congestion in case of an extended SCADA master outage.
- **Unsolicited Transmit Delay Event Count.** This is the maximum number of DNP3 unsolicited events the gateway will queue before sending to the SCADA master. A value of one (1) disables the queuing mechanism so the gateway will immediately send all unsolicited events.

- **Unsolicited Transmit Delay Time.** This is the maximum amount of time the gateway will queue DNP3 unsolicited events before sending to the SCADA master, in units of milliseconds. This complements the **Unsolicited Transmit Delay Event Count** field. When the number of queued events reaches the **Unsolicited Transmit Delay Event Count** setting or the time since the first event was queued reaches the **Unsolicited Transmit Delay Time** setting, whichever comes first, the queued events are transmitted.

## DNP3 Setpoints Settings

In this panel, all setpoint types will be defined and mapped. A full list of code-description definitions is found in S&C Instruction Sheet 461-560, “TripSaver® II Communications Gateway: *DNP Points List and Implementation.*”

The process to make point changes for each category (Analog Inputs, Counters, and Binary Outputs) is identical. In the next section, there will be a detailed overview of how to set a Status (Binary Input) point. Screen captures will not be provided for each process step for the Analog Input, Counter, and Binary Output categories.

## Status (Binary Input) Points Configuration

This window contains configuration parameters for DNP binary inputs. The window is initiated by clicking on the **Status (Binary Input)** button. See Figure 59.

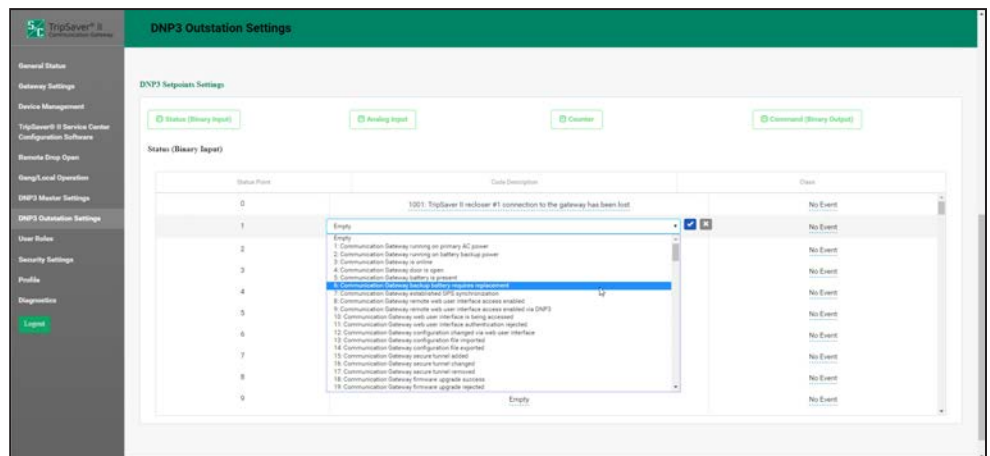


Figure 59. The Status (Binary Input) point entry field.

# Configuring the Communications Gateway

**Status Point:** These point numbers represent what the SCADA system will see in response to a static or event data request or an unsolicited event response.

**Code Description:** Point codes representing specific status points may be assigned to individual SCADA point numbers. A full list of code-description definitions is found in S&C Instruction Sheet 461-560, “TripSaver® II Communications Gateway: *DNP Points List and Implementation.*” Code descriptions are defined by selecting the **Code Description** field in line with the respective **Status Point** field. A drop-down dialog box will appear with code definitions for all TripSaver II reclosers paired with the communications gateway. See Figure 60. When a code definition has been chosen, select the **Check Mark** icon to finalize it. Removal of a code selection can be performed by selecting the blank row in the pull-down menu and clicking on the check mark. This will result in the field being displayed as empty. Finally, click on the **Save** button.

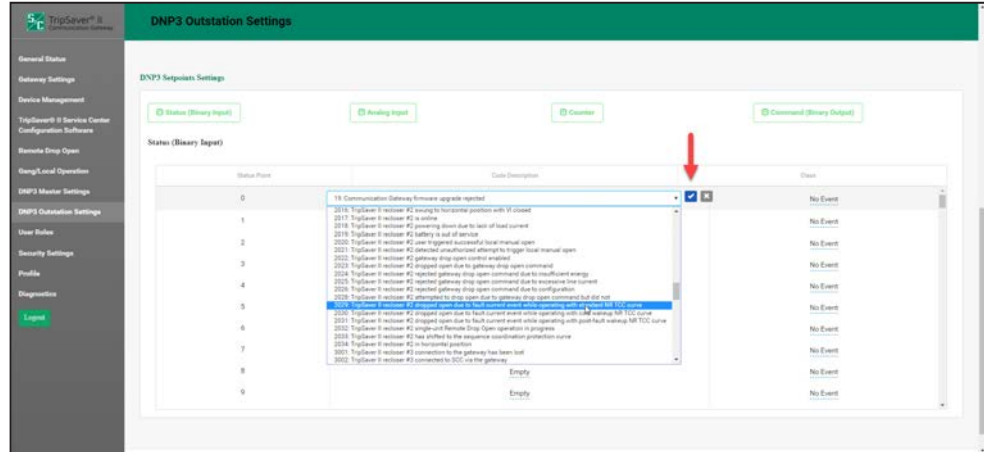


Figure 60. The Code Description drop-down menu.

**Class:** This is the DNP event class in which this point can be placed. Specify Class 1, Class 2, or Class 3, or choose the **No Event** option if event data reporting is turned off for that point.



Follow these steps to input the settings:

- STEP 1.** Navigate to the field on the Status Point line.
- STEP 2.** Initiate the drop-down menu by selecting the field.
- STEP 3.** Highlight the desired identifier.
- STEP 4.** Select the check mark for acknowledgement.
- STEP 5.** After all points are mapped, click on the **Save** button at the top of the screen.

Figure 61 shows an example of Status Point 1 after being saved to the communications gateway.

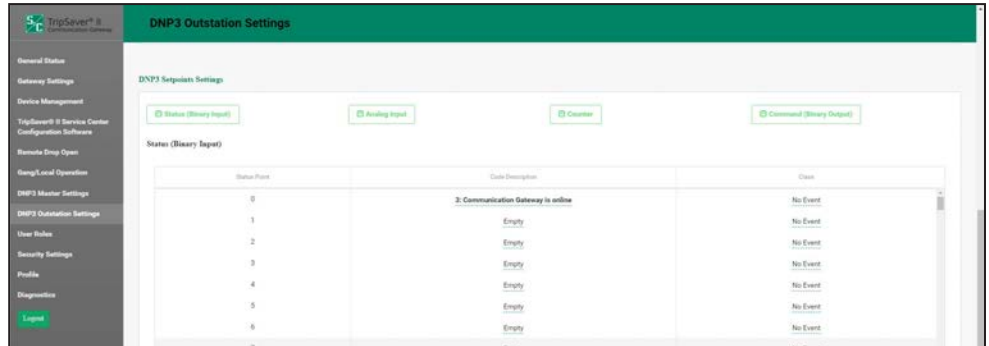


Figure 61. A completed Status Point entry.

## Analog Input Points Configuration

This window contains configuration parameters for analog input points. Mapping these points will make them available in SCADA. The window is initiated by clicking on the **Analog Input** button. See Figure 62.

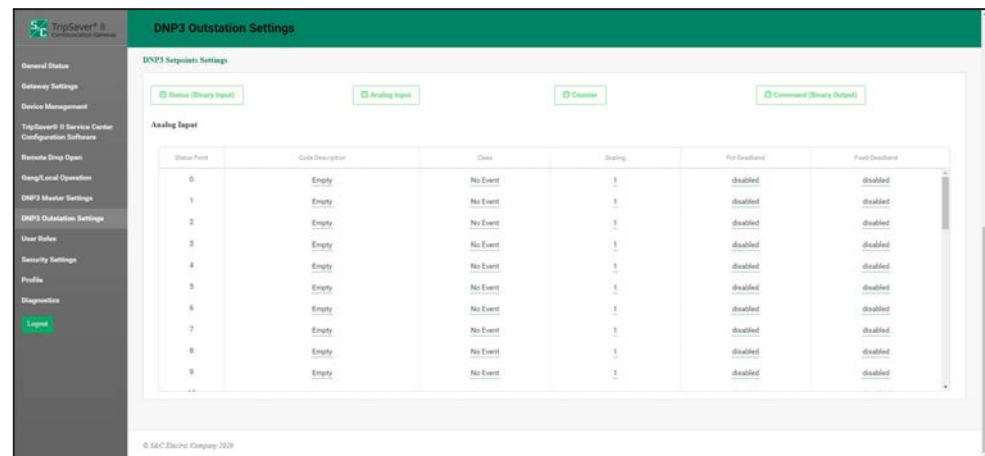


Figure 62. The *Analog Input Points* configuration screen.

**Status Point:** These point numbers represent what the SCADA system will see in response to a static or event data request or an unsolicited event response.

**Code Description:** These are the point codes representing specific analog inputs that may be assigned to individual SCADA point numbers for TripSaver II reclosers paired with a communications gateway. A full list of code-description definitions is found in S&C Instruction Sheet 461-560, “TripSaver® II Communications Gateway: *DNP Points List and Implementation*.” Code descriptions are defined by selecting the **Code Description** field in line with the respective **Status Point** field. A drop-down dialog box will appear with code definitions for all TripSaver II reclosers paired with the communications gateway. When a code definition has been chosen, select the **Check Mark** icon to finalize it. Removal of a code selection can be performed by selecting the blank row in the pull-down menu and clicking on the check mark. This will result in the field being displayed as empty. Finally, click on the **Save** button.

**Event Class:** This is the DNP event class assigned to this point. Specify Class 1, Class 2, or Class 3, or choose the **No Event** option to turn off event-data reporting for this point.

**Scaling:** A scaling factor is used for the analog input data to match the analog input requirements of the SCADA system. The original raw analog input data will be multiplied by the specified scaling factor prior to delivery to the SCADA master. If the **Fixed Deadband** option is enabled for an analog input setpoint, the scaling factor will be applied before the Fixed Deadband limits are checked.

**Pct (Percent) Deadband:** This field creates a range based on a percentage of the last reported value for this analog input. The range boundary is defined by multiplying the field input value by the value of the analog point. In the case where the next analog input “READ,” specific to this point, exceeds the range either by a positive or negative amount, the information will be included in the next event report. The default value is **Disabled**. No range is created and no comparison occurs. Specifying a **Zero** value or any other number creates the range and enables the comparison. To disable this field, select the **Blank Row** option in the pull-down menu to switch back to **Disabled** mode.

**Fixed Deadband:** This field creates a fixed deadband range relative to the last reported value for this analog input. If the next analog input “READ,” specific to this point, exceeds the range either by a positive or negative amount, the information will be included in the next event report. The default value is **Disabled**. No range is created, and no comparison occurs. Specifying a **Zero** value or any other number creates the range and enables the comparison. To disable this field after it has been enabled, select the **Blank Row** option in the pull-down menu to switch back to **Disabled** mode.

### Counter Points Configuration

This window contains configuration parameters for counter points. Mapping these points will make them available in SCADA. The window is initiated by clicking on the **Counter** button. See Figure 63.

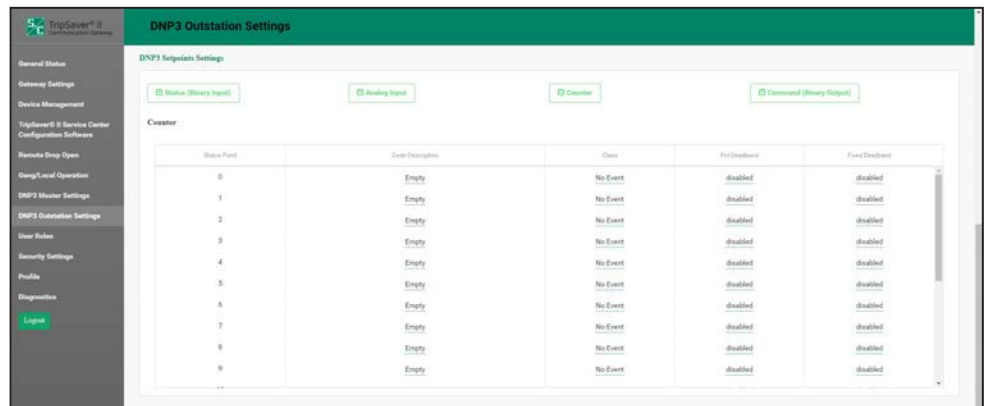


Figure 63. The Counter Points configuration screen.

**Status Point:** This is the point number the SCADA system will see in response to a static or event data request or an unsolicited response.

**Code Description:** This point code represents a specific type of counter reported by the TripSaver II recloser. There are counter points for each of the four TripSaver II reclosers. A full list of code-description definitions is found in S&C Instruction Sheet 461-560, "TripSaver® II Communications Gateway: *DNP Points List and Implementation.*"

Code descriptions are defined by selecting the **Code Description** field in line with the respective **Status Point** field. A drop-down dialog box will appear with code definitions for all TripSaver II reclosers paired with the communications gateway. When a code definition has been chosen, select the **Check Mark** icon to finalize it. Removal of a code selection can be performed by selecting the blank row in the pull-down menu and clicking on the check mark. This will result in the field being displayed as empty. Finally, click on the **Save** button.

**Class:** This is the DNP event class in which this point can be placed. Specify Class 1, Class 2, or Class 3, or chose the **No Event** option to turn off event data reporting for this field.

**Pct (Percent) Deadband:** This field creates a range based on a percentage of the last reported value for this counter point. The range bound is defined by multiplying the field input value by the value of the counter point. In the case where the next analog input "READ," specific to this point, exceeds the range either by a positive or negative amount, the information will be included in the next event report. The default value is **Disabled**. No range is created and no comparison occurs. Specifying a Zero value or any other number creates the range and enables the comparison. To disable this field after it has been enabled, select the **Blank Row** option in the pull-down menu to switch back to **Disabled** mode.

**Fixed Deadband:** This field creates a fixed deadband range relative to the last reported value for this counter point. If the next counter input "READ," specific to this point, exceeds the range either by a positive or negative amount, the information will be included in the next event report.

The default value is **Disabled**. No range is created, and no comparison occurs. Specifying a Zero value or any other number creates the range and enables the comparison. To disable this field after it has been enabled, select the **Blank Row** option in the pull-down menu to switch back to **Disabled** mode.

## Command (Binary Output) Points Configuration

This window contains configuration parameters for command point mapping. See Figure 64. Mapping these points will make them available in SCADA.

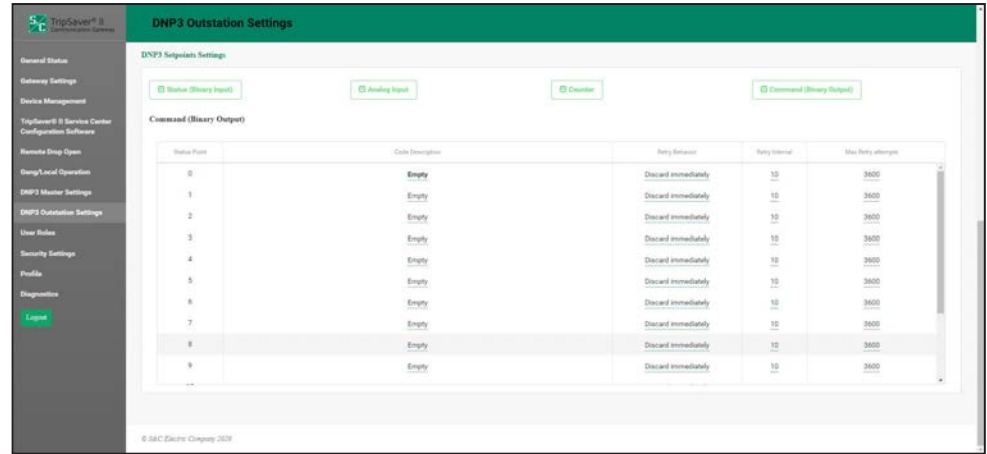


Figure 64. The **Command (Binary Output)** configuration screen.

**Status Point:** This is the point number the SCADA system will use when operating the command point.

**Code Description:** Binary outputs are used by the SCADA master to update settings in the communications gateway or any of the associated TripSaver II reclosers. A full list of code-description definitions is found in Instruction Sheet 461-560, “TripSaver® II Communications gateway: *DNP Points List and Implementation.*”

Code descriptions are defined by selecting the **Code Description** field in line with the respective **Status Point** field. A drop-down dialog box will appear with code definitions for all TripSaver II reclosers paired with the communications gateway. When a code definition has been chosen, select the **Check Mark** icon to finalize it. Removal of a code selection can be performed by selecting the blank row in the pull-down menu and clicking on the check mark. This will result in the field being displayed as empty. Finally, click on the **Save** button.

Follow these steps to complete the process:

- STEP 1.** Navigate to the field on the status point line.
- STEP 2.** Initiate respective drop-down boxes by selecting the field.
- STEP 3.** Highlight the identifier.
- STEP 4.** Select the check mark for acknowledgement.
- STEP 5.** After all points are mapped, click on the **Save** button.

**Retry Behavior:** This drop-down menu allows one of two selections. The **Discard Immediately** setting will ignore the **Retry Interval** and **Max Retry Attempts** settings the **Command (Binary Output)** point will not retry. The **Queue/Retry for a Specified Count** setting will retry the send for the specified **Retry Interval** and **Max Retry Attempts** settings.

**Retry Interval:** This is the interval between retries. (Range: 1 to 3600)

**Max Retry Attempts:** This is the maximum number of retry attempts that will be sent. (Range: 1 to 2,592,000)

### User Roles

The purpose of the **User Roles** menu is for adding users and corresponding access privileges. The types of user roles include Admin, Gateway User, TripSaver II User, and Technician. The addition of a user is initiated by clicking on the **Add User** button. A dialog box will open with the required **User**, **Password**, and **Confirm Password** fields, and a drop-down box to select user type. See Figure 65.

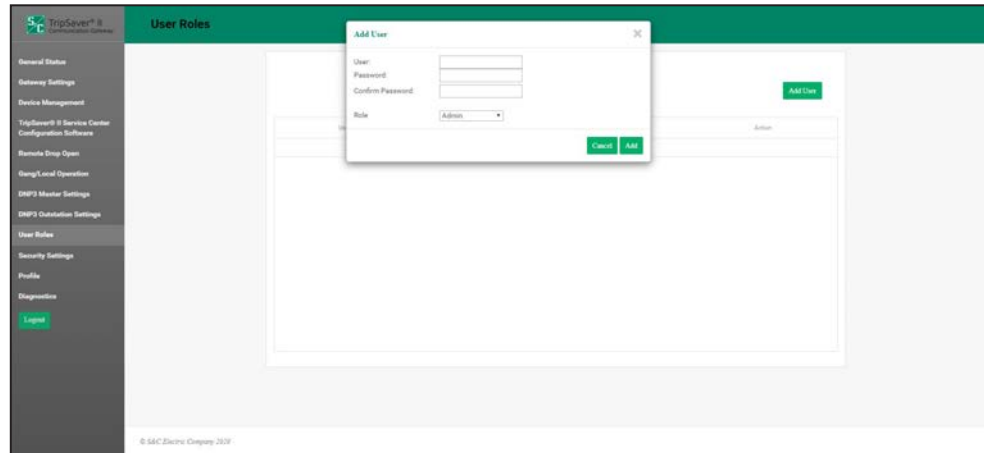


Figure 65. The *User Role* configuration screen.

The permissions provided to each of the user roles is summarized in Table 3.

**Table 3. User Role Permissions**

Page	Element Within Screen	Admin Role	Gateway User Role	TripSaver II User Role	Technician Role
General Status	All	Allowed	Allowed	Allowed	Allowed
Gateway Settings	Update gateway configuration	Allowed	Allowed	Blocked	Blocked
	Install firmware	Allowed	Blocked	Blocked	Blocked
Device Management	Add/Update/Remove TSII buttons	Allowed	Allowed	Allowed	Blocked
	Display TripSaver II recloser status	Allowed	Allowed	Allowed	Blocked
Remote Drop Open	All	Allowed	Blocked	Blocked	Blocked
Gang/Local Operation	Configure gang operation settings	Allowed	Allowed	Blocked	Blocked
	Perform Gang Trip/Cancel Gang Trip buttons	Allowed	Blocked	Blocked	Blocked
TripSaver II Service Center Configuration Software	All	Allowed	Blocked	Allowed	Blocked
DNP3 Master Settings	All	Allowed	Allowed	Blocked	Blocked
DNP3 Outstation Settings	All	Allowed	Allowed	Blocked	Blocked
User Roles	All	Allowed	Blocked	Blocked	Blocked
Security Settings	Configure secure tunnel	Allowed	Allowed	Blocked	Blocked
	Provision HTTPS server certificate	Allowed	Allowed	Blocked	Blocked
	Enable remote web UI access	Allowed	Blocked	Blocked	Blocked
Profile	All	Allowed	Allowed	Allowed	Allowed
Diagnostics	All	Allowed	Allowed	Allowed	Allowed

## Security Settings

### Secure Tunnel

The communications gateway supports the ability to tunnel all communication network traffic from the communications gateway to a customer-supplied peer. See Figure 66. Enabling a secure tunnel from the communications gateway creates an authenticated, encrypted, and integrity-protected path through which DNP3 traffic will pass.

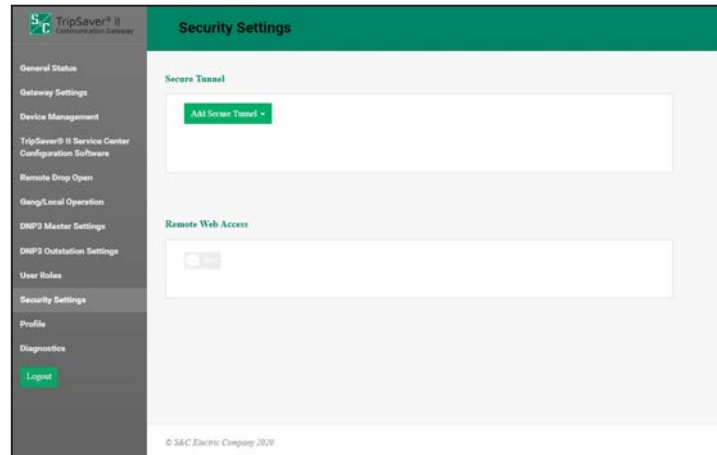


Figure 66. The Secure Tunnel toggle button.

In the **Security Settings** menu, the communications gateway administrator can create the secure communication **OpenVPN** option.

To create a secure tunnel, click on the **Add Secure Tunnel** button and select the **Open VPN** option from the drop-down menu. A dialog box will appear for field entry. When the fields are completed, click on the **Add** button to complete and add the tunnel profile. See Figure 67 on page 71.



## OpenVPN Configuration

This type of security tunnel allows the administrator to create an OpenVPN tunnel to encapsulate IP packets from the local interface to the remote OpenVPN server.

As with the tunnel configuration above, select the **Open VPN** option from the drop-down menu. A configuration dialog box will appear. See Figure 67.

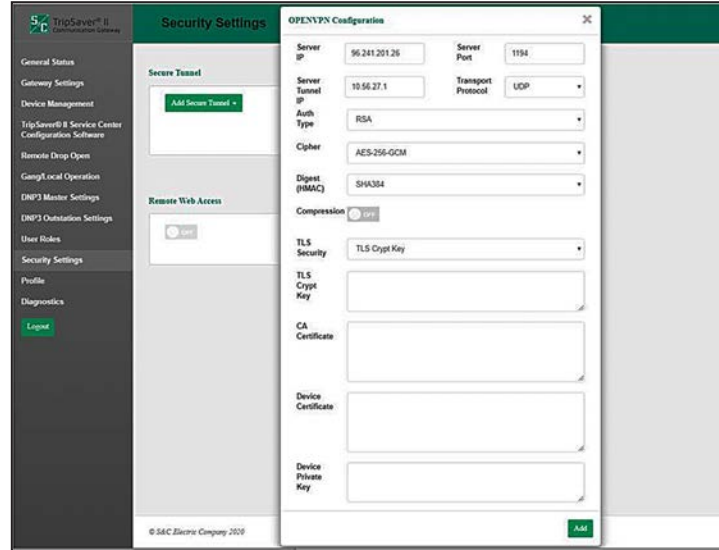


Figure 67. The Open VPN configuration menu.

Follow these steps to add OpenVPN:

- STEP 1.** Enter the IP (private) address of the VPN server in the **IPsec Server IP** field.
- STEP 2.** Enter the Server port number into the **Server Port** field.
- STEP 3.** Enter the (private) IP address into the **Server Tunnel IP** field.
- STEP 4.** Select either UDP or TCP transport protocol for the **Transport Protocol** field.
- STEP 5.** Choose a selection, either 128 or 256 AES Cipher key, from the **Cipher** drop-down menu.
- STEP 6.** Choose a selection from the **Digest (HMAC)** drop-down menu.
- STEP 7.** Select either the **On** or **Off** setting for data compression by selecting the **Compression** field.
- STEP 8.** Choose a selection from the **TLS Security** drop-down menu.
- STEP 9.** Enter a key in the **TLS Crypt Key** field.
- STEP 10.** Enter the CA certificate into the **CA Certificate** field.
- STEP 11.** Enter the device certificate into the **Device Certificate** field.
- STEP 12.** Enter the device private key into the **Device Private Key** field.
- STEP 13.** Click on the **Add** button to complete tunnel addition.

The configured OpenVPN tunnel will appear in the listing. Tunnel deletions and modifications are managed by selecting the buttons in this listing.

### Remote Web Access

The **Remote Web Access** toggle button enables Web-user interface access via Ethernet Port 2. This configuration setting can only be updated by the admin user and only after the admin user has changed the default password. Web access via Ethernet Port 2 is also controlled by a **DNF3 binary output** setpoint, which must also be enabled to allow this traffic. See Figure 68. See the “Enabling Remote Web Access on page 73.

#### NOTICE

If a SpeedNet™ Radio is being used for the field area network radio, the remote Web user's computer will require an additional setting to be updated to enable Web access. The user must reduce the MTU (maximum transmission unit) size to a value of 500 or lower. S&C recommends using an MTU size of 500 for optimal performance. To change the MTU size, the following command can be used on a Windows 10 machine: **netsh interface ipv4 set subinterface "Local Area Connection" mtu=500 store=persistent.**

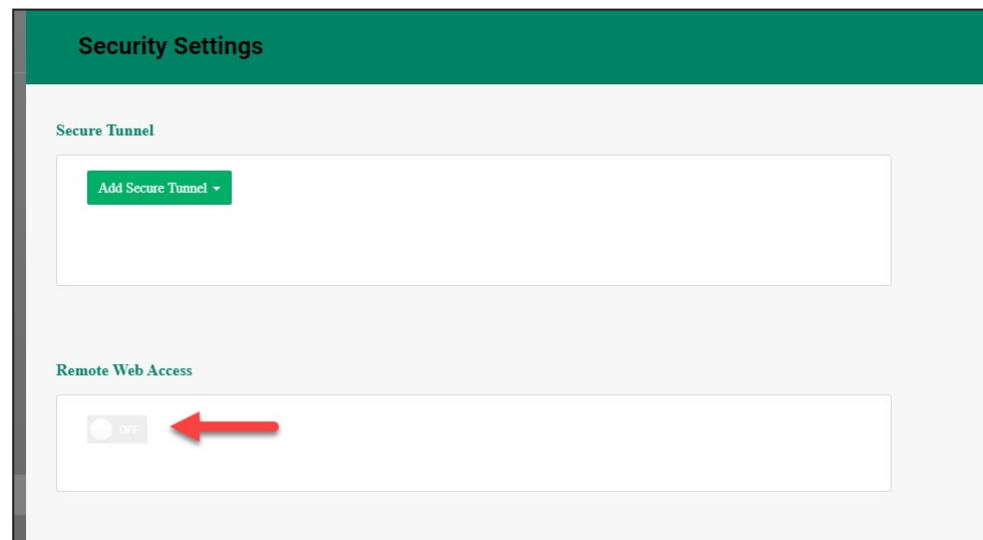


Figure 68. The Remote Web Access toggle button.

## Enabling Remote Web Access

### NOTICE

The **Remote Web Access** feature provides similar functionality to local access via Ethernet Port 1. There are some limitations when accessing the Gateway via the **Remote Web Access** feature:

- The **Drop Open** commands on the *Gang/Local Operation* screen will not be available.
- The **Enable** command on the *TripSaver II Service Center Configuration Software* screen will not be available.

Follow these steps to enable the **Remote Web Access** feature:

**STEP 1.** On the *Profile* screen, the gateway admin password must be changed locally from the default password.

**STEP 2.** On the *Security Settings* screen, the **Remote Web Access** function must be set to the **On** position. See Figure 69.

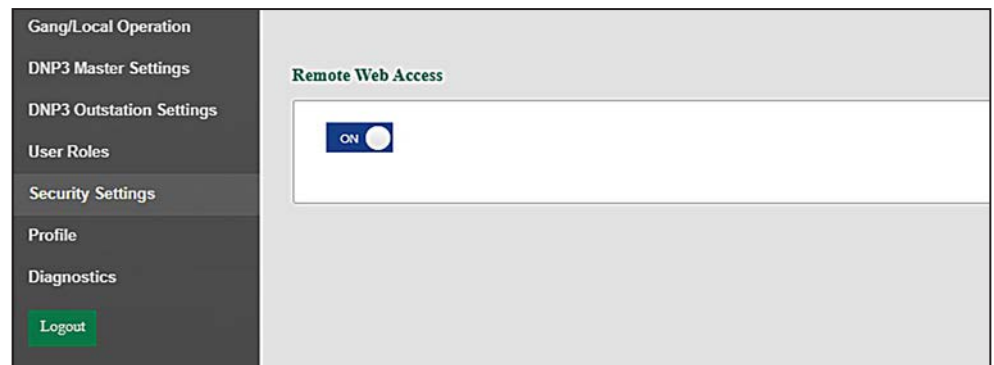


Figure 69. The Remote Web Access slide selector.

## Configuring the Communications Gateway

**STEP 3.** On the *DNP3 Outstation Settings* screen, **Command (Binary Output)** field, a Binary Output status point must be configured with code description “1: Communication Gateway remote web user interface switch.” See Figure 70.

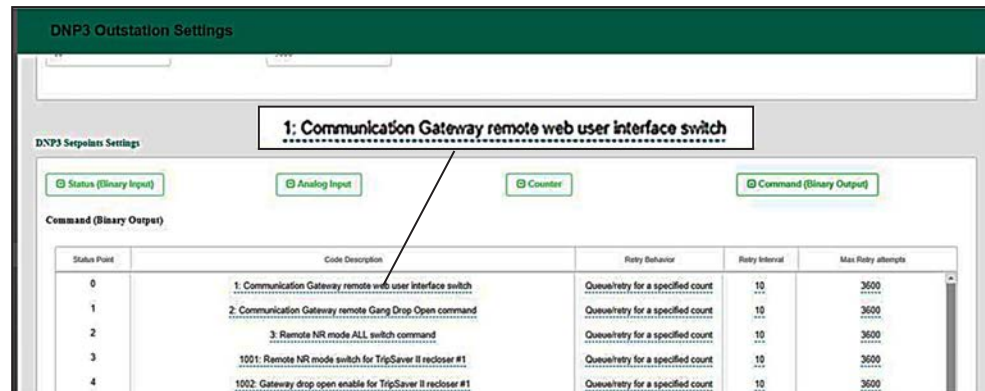


Figure 70. Configuring the Remote Web UI DNP3 command (binary output).

**STEP 4.** See Figure 71. On the *DNP3 Outstation Settings* screen, **Status (Binary Input)** field, two Binary Input status points must be configured with the following code descriptions:

“8. Communication Gateway remote web user interface access enabled”

“9. Communication Gateway remote web user interface access enable via DNP3”

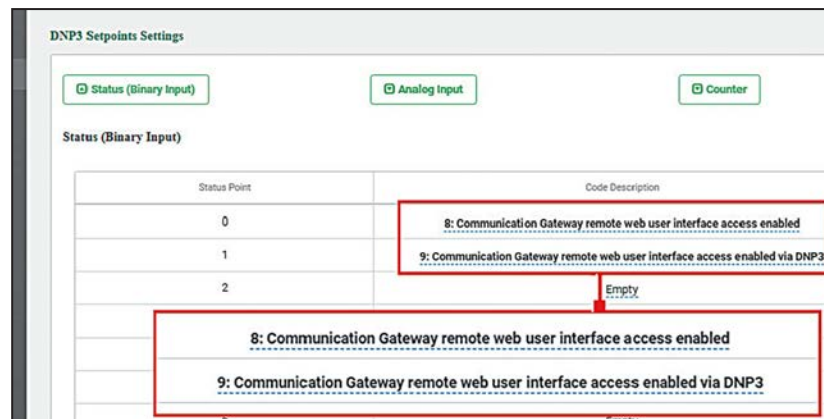
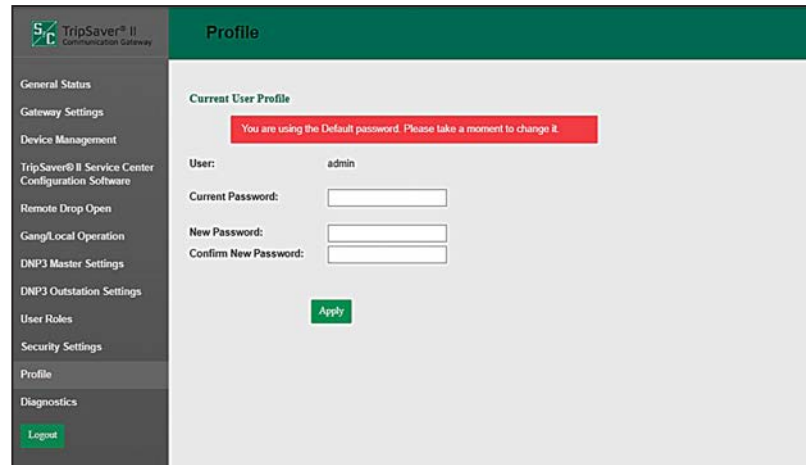


Figure 71. Configuring the Remote Web UI DNP3 status points (binary inputs).

- STEP 5.** If a SpeedNet™ Radio is used for the field area network radio, the remote Web user's computer will require an additional setting to be updated to enable Web access. The user must reduce the MTU (maximum transmission unit) size to a value of 500 or lower. S&C recommends using an MTU size of 500 for optimal performance. To change the MTU size, the following command can be used on a Windows 10 machine: **netsh interface ipv4 set sub-interface "Local Area Connection" mtu=500 store=persistent.**
- STEP 6.** From the DNP3 Master/SCADA Master, send the following command to the status point configured in STEP 3 on page 74:
- Direct Relay control command
  - (a) Type = Latching Relay
  - (b) Value = Latch On (To Enable)
- STEP 7.** Check the Binary Input status points that align with the status points configured in STEP 4 on page 74.
- 8: Communication Gateway remote web user interface access enabled status point reflects "1"/"True" value
  - 9: Communication Gateway remote web user interface access enabled via DNP3 status point reflects "1"/"True" value
- STEP 8.** When the Binary Input status points reflect the values in Step 7, the user should confirm connectivity to the communication gateway from the user's computer configured with the workaround and connected into the network connected to the SpeedNet Radio headend point.
- URL: IP address associated with communication gateway's Ethernet Port 2.

## Profile

The *Profile* screen enables the present user logged in to the communication gateway to change their password credentials. See Figure 72.



The screenshot shows the 'Profile' screen of the TripSaver II Communication Gateway. The left sidebar contains a navigation menu with the following items: General Status, Gateway Settings, Device Management, TripSaver® II Service Center Configuration Software, Remote Drop Open, Gang/Local Operation, DNP3 Master Settings, DNP3 Outstation Settings, User Roles, Security Settings, Profile (highlighted), and Diagnostics. At the bottom of the sidebar is a 'Logout' button. The main content area is titled 'Profile' and displays the 'Current User Profile' for the user 'admin'. A red warning banner at the top of the main area reads: 'You are using the Default password. Please take a moment to change it.' Below this, there are three input fields: 'Current Password:', 'New Password:', and 'Confirm New Password:'. An 'Apply' button is located below the input fields.

**Figure 72.** The *Profile* screen.

## Diagnostics

The purpose of the *Diagnostics* screen is to initiate the retrieval of the Diagnostic and Event Log files. See Figure 73.

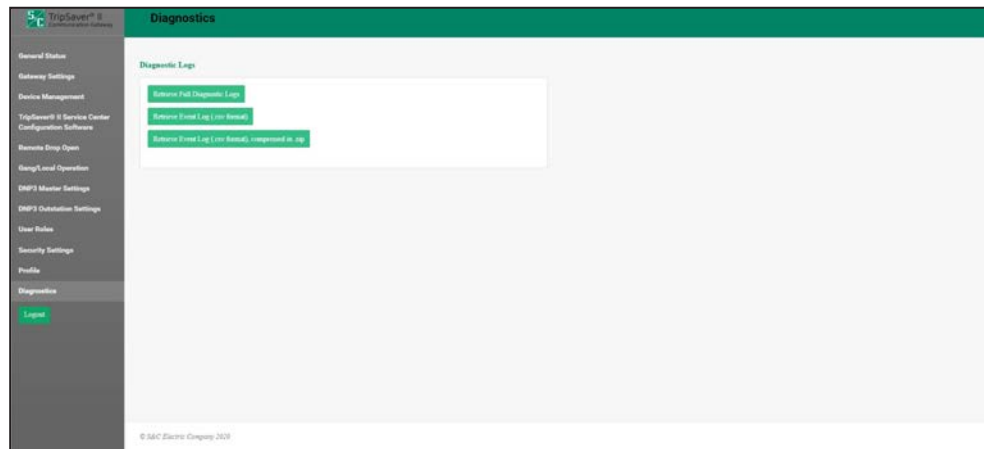


Figure 73. The *Diagnostics* screen retrieves files.

When the **Retrieve** button is selected, a dialog box appears notifying the user of the file-retrieval interval. See Figure 74.

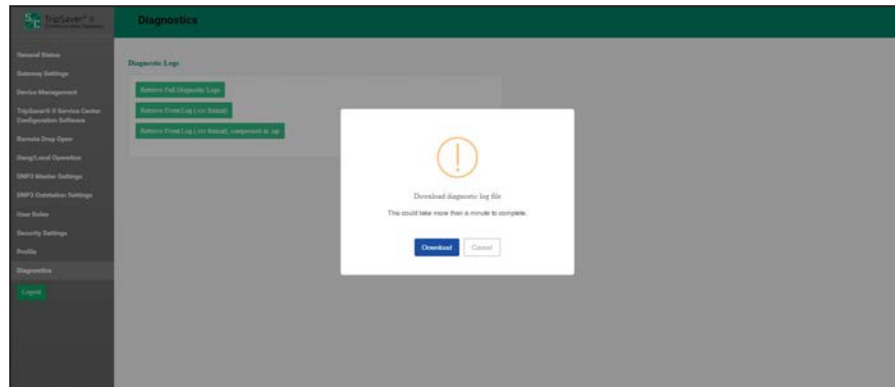


Figure 74. The Diagnostic Log retrieval interval dialog box.

If the **Download** button is clicked, a notification of file download completion appears, and the Log file will be saved in the computer's Download file folder. See Figure 75.

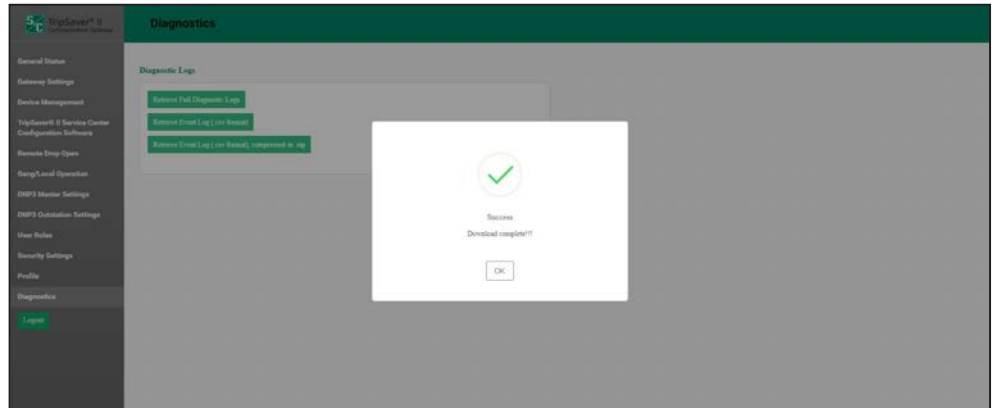


Figure 75. The Diagnostic Log completion dialog box.

## Commissioning (Pairing) a TripSaver II Recloser for Use with the Communications Gateway

### Service Center Pairing a TripSaver II Recloser with Firmware Version 1.8 or Later

#### NOTICE

A guide to pairing your TripSaver II recloser with the communications gateway can also be found in S&C Instruction sheet 461-521, "TripSaver® II Cutout-Mounted Recloser, Outdoor Distribution (15 kV and 25 kV): *TripSaver® II Communications via Gateway Pairing Quickstart Guide.*"

#### DANGER

The TripSaver II Cutout-Mounted Recloser **MUST** be de-energized and removed from the utility pole before attaching the "corded" power module (power module with ac adapter and extension cord) to the base of the TripSaver II recloser. The corded power module is **ONLY** intended to be used for setup and data collection when the TripSaver II recloser is de-energized and removed from the utility pole. Failure to remove the TripSaver II recloser from the utility pole before connecting the corded power module can cause arcing, burns, electric shock, and death.

With the introduction of TripSaver II Cutout-Mounted Recloser firmware version 1.8 or later, the TripSaver II recloser can be paired with a communications gateway at the user's service center using the power module from the service center configuration kit and the S&C Magnet Tool. S&C recommends commissioning (pairing) TripSaver II reclosers with the communications gateway one at a time. This will ensure each recloser is fully connected to the communications gateway before pairing the next recloser. Pairing the reclosers one at a time is the fastest method to pair a TripSaver II recloser and a communications gateway. TripSaver II reclosers must be furnished with the **Extended Open Interval** option, which allows up to a 30-second open interval between reclose operations.

To pair a TripSaver II recloser in the service center:

- STEP 1.** Using a PC loaded with Service Center Configuration Software, the corded power module, a USB transceiver, and TripSaver II Service Center Configuration Software, set the TripSaver II recloser loaded with firmware version 1.8 or later to **Gateway** mode. Instructions for setting the recloser to **Gateway** mode can be found in the "Communications Settings Menu" section of S&C Instruction Sheet 461-504, "TripSaver® II Cutout-Mounted Recloser, Outdoor Distribution (15 kV and 25 kV): For Overhead Distribution Systems: *Protection Setup Using Service Center Configuration Kit.*"
- STEP 2.** Disconnect from the service center configuration software and remove the USB transceiver from the PC. With the power module still connected to the TripSaver II recloser, attach the magnet tool's magnet to the green S&C logo sticker on the side of the TripSaver II recloser. More information on using the Magnet Tool can be found in S&C Instruction Sheet 461-507, "TripSaver® II Cutout-Mounted Recloser, Outdoor Distribution (15 kV and 25 kV): *Operation Manual Enabling Pole-Top Communications Via the Magnet Tool.*" This will turn on the TripSaver II recloser's wireless communications.



**STEP 3.** Connect to the communications gateway with a PC as described in the “Software User’s Guide” section on page 19. In the *Device Management* screen, click on the **Add TripSaver II** button. Fill in the Transceiver ID and TripSaver II Device Name (if desired) and click on the **OK** button.

**Note:** The device name can be anything but is usually a description of where the TripSaver II recloser is installed.

When the TripSaver II recloser has been successfully paired, the device will appear in the device listing in the device panel. Periodically refresh the communications gateway’s *TripSaver II Device Management* screen using your browser’s **Refresh** button. The TripSaver II recloser will be listed as “connected” when pairing is complete. The pairing process could take approximately 5 minutes. If the TripSaver II recloser does not pair, see the “Troubleshooting” section on page 81.

**STEP 4.** When paired, disconnect the magnet tool’s magnet and the power module. Both the communications gateway and TripSaver II Recloser will remember their pairing after being moved to the installation site and installed. The paired TripSaver II reclosers should be installed no more than 100 feet (30.5 m) from the communications gateway. For optimal performance, install the TripSaver II recloser no more than 30 feet (9.1 m) away from the communications gateway and in direct line of sight.

## Field Pairing a TripSaver II Recloser with Firmware Version 1.6 or 1.7 Installed on the Utility Pole and Powered by Line Current

For TripSaver II reclosers furnished with firmware version 1.6 or 1.7, pairing can only be performed with the TripSaver II recloser powered by line current or an external power source. (For specifications for an external power source, contact the S&C Global Support and Monitoring Center.) To pair with the communications gateway, these reclosers must be installed within 100 feet (30.5 m) of the communications gateway and be furnished with the **Extended Open Interval** option, which allows up to a 30 second open interval between reclose operations.

**Note:** Though S&C strongly recommends upgrading the firmware of the TripSaver II recloser to be paired with the communications gateway to version 1.9, there may be a need to pair a TripSaver II recloser using an older version of the firmware with a communications gateway. For TripSaver II reclosers furnished with firmware version 1.6 or 1.7, pairing can only be performed at the installation site with the TripSaver II recloser powered by line current. This procedure can also be used when pairing a TripSaver II recloser with firmware versions 1.8 or later with a communications gateway already installed in the field.

To perform field pairing, follow these steps:

**STEP 1.** Using a PC loaded with Service Center Configuration Software v1.8, the corded power module, a USB transceiver, and TripSaver II Service Center Configuration Software, set the TripSaver II recloser to **Gateway** mode. Instructions for setting the recloser to **Gateway** mode can be found in the “Communications Settings Menu” section of S&C Instruction Sheet 461-504, “TripSaver® II Cutout-Mounted Recloser, Outdoor Distribution (15 kV and 25 kV): For Overhead Distribution Systems: *Protection Setup Using Service Center Configuration Kit.*” Disconnect the service center configuration software and remove the USB transceiver from the USB port.

## Commissioning (Pairing) a TripSaver II Recloser for Use with the Communications Gateway

---

- STEP 2.** Install the TripSaver II recloser(s) to be paired to the gateway to the utility pole as described in S&C Instruction Sheet 461-502, “TripSaver® II Cutout-Mounted Recloser, Outdoor Distribution (15 kV and 25 kV): *Installation and Operation*,” and power it via line current. Install the communications gateway no more than 30 feet (9.1 m) from the TripSaver II recloser(s) to be paired. Connect the communications gateway to ac power.
- STEP 3.** Connect to the communications gateway with a PC as described in the “Software User’s Guide” section on page 19. In the *Device Management* screen, click on the **Add TripSaver II** button. Fill in the Transceiver ID and TripSaver II Device Name (if desired), and click on the **OK** button.

**Note:** The device name can be anything but is usually a description of where the TripSaver II recloser is installed.

When the TripSaver II recloser has been successfully paired, the device will appear in the device listing in the device panel. Periodically refresh the communications gateway’s *TripSaver II Device Management* screen using the browser’s **Refresh** button. The TripSaver II recloser will be listed as “connected” when pairing is complete. The pairing process could take approximately 15 minutes. If the TripSaver II recloser does not pair, see the “Troubleshooting” section on page 81.

**Signal Interference**

Difficulties in pairing a TripSaver II recloser with a communications gateway are usually caused by signal interference. Remember, the communications gateway should be no more than 100 feet (30.5 m) away from the TripSaver II recloser and should have an unobstructed view of the recloser. The communications gateway antenna is directional, and the TripSaver II reclosers must be installed above the communications gateway, ideally on the same pole. Also, the heavy use of Bluetooth devices, cellular devices, or Wi-Fi can cause radio interference.

If radio traffic is heavy, S&C recommends moving the recloser and communications gateway closer to one another.

For optimal performance, install the TripSaver II recloser no more than 30 feet (9.1 m) away from the communications gateway and in direct line of sight.

**Pairing Process Takes Longer Than Expected**

Pairing a TripSaver II Cutout-Mounted Recloser should take approximately 5 minutes. In some cases, it may take up to 15 minutes. If after waiting for 15 minutes the gateway (after refreshing the browser) does not register as “connected,” S&C recommends resetting wireless communications in the TripSaver II recloser by completing the following procedure:

- STEP 1.** Mitigate any signal interference using the techniques described in the “Signal Interference” section.
- STEP 2.** With the recloser removed from the utility pole, connect to the TripSaver II recloser using the service center configuration kit. (The kit includes the USB transceiver, corded power module, and ac adapter.) Detailed Instructions for connecting to a TripSaver II recloser using the Service Center Configuration Software can be found in S&C Instruction Sheet 461-504, “TripSaver® II Cutout-Mounted Recloser, Outdoor Distribution (15 kV and 25 kV): For Overhead Distribution Systems: *Protection Setup Using Service Center Configuration Kit.*”
- STEP 3.** Navigate to the *Communications Settings* screen and select the Communications Mode drop-down menu. Change the **Communications mode** to the **Non-Gateway Mode** setting.
- STEP 4.** Click on the **Apply Communications Mode** button.  
**Note:** The **Apply Communications Mode** button will not apply any changes that have been made on any other menu screens. If changes have been made to another menu screen, such as the *TCC Curve Settings* screen, click on the **Apply** button.
- STEP 5.** The TripSaver II recloser is now in **Non-Gateway** mode. Select **Gateway** mode from the drop-down menu. Click on the **Apply Communications Mode** button to place the recloser back in **Gateway** mode.
- STEP 6.** Connect to the communications gateway, as described in the “Software User’s Guide” section on page 19. Remove the TripSaver II recloser’s entry on the *Device Management* screen. Disconnect the TripSaver II recloser from the service center configuration software by clicking on the **Disconnect** button.
- STEP 7.** Pair the TripSaver II recloser with the new communications gateway using the instructions in the “Commissioning (Pairing) a TripSaver II Recloser for Use with the Communications Gateway” section on page 78.

## Quick Installation Checklist

---

### **Pre-Installation**

- Examine the shipment(s) and make sure it includes:
  - The communications gateway
  - Mounting hardware for securing the gateway to the pole
  - An ac power cable

Also, make sure the recloser uses firmware v1.6 or later for **Extended Open Interval** functionality.

- Always read the Danger and Warning labels.
- Follow your company's PPE guidelines and standard operating procedures.

### **Installation**

- For the communications gateway, verify that:
  - The field-area-network radio is configured, installed, and connected.
  - The communications gateway is mounted securely on the pole.
  - The communications gateway is grounded.
  - The ac power cable is connected and control power is available.
  - The remote antenna (if applicable) is installed and connected.
  - The communications gateway is locked for security, when configured and operational.
  
- For the TripSaver II reclosers, verify that:
  - The recloser is set to **Gateway** mode.
  - The reclosers are powered.

After the above steps are complete, proceed with the following if they have not already been done:

- Pair the communications gateway with TripSaver II recloser(s).
- Configure the communications gateway. To configure the communications gateway in the service center, use the three-prong ac power cable (cat. number 007-002101-01/02).

## Interface Pinouts

The RS-232 port of the gateway controller module (green box) is configured as data-terminal equipment. See Table 4.

**Table 4. Gateway Controller Module RS-232 Interface Pinout**

Pin	Function	Description
1	NC	No Connection
2	RX from Radio	RS-232 Receive
3	TX to Radio	RS-232 Transmit
4	NC	No Connection
5	TX to Radio GND	Signal Ground
6	NC	No Connection
7	RTS to Radio	Request to Send
8	CTS to Radio	Clear to Send
9	NC	No Connection

Ethernet Ports 1 and 2 use RJ-45 connectors with the pinout shown in Table 5. They are auto-sensing for assignment of transmit and receive lines (no crossover cables required) and auto-negotiate for 10-mbps or 100-mbps data rates, as required by the connected device.

**Table 5. Ethernet Ports Pinout**

Pin	Function	Description
1	TXD+	Transmit
2	TXD-	Transmit
3	RXD+	Receive
4	NC	No Connection
5	NC	No Connection
6	RXD-	Receive
7	NC	No Connection
8	NC	No Connection

Power System  
Diagram

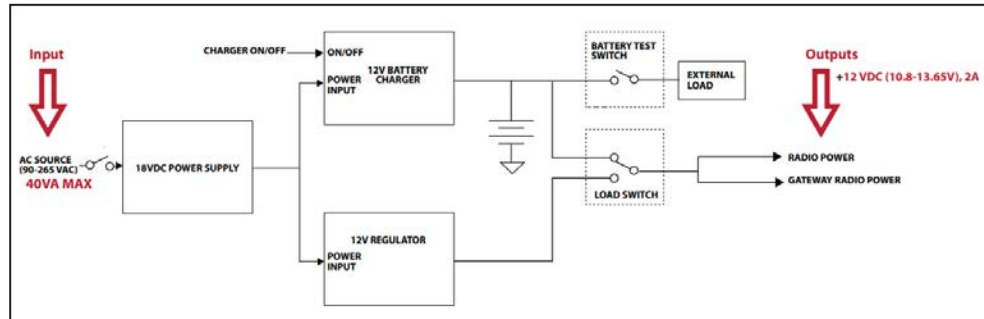


Figure 76. The communications gateway power system diagram.

**Note:** A user-supplied disconnect switch may be required for installation between the ac input and the PS/battery board. Contact your nearest S&C Sales Office for details.

## Understanding the Radio Mode

The TripSaver II recloser has a built-in transceiver for local communications that can be operated in one of two radio modes: USB Transceiver mode or Communications Gateway mode. Both modes use short-range 2.4-GHz wireless communications. With a USB transceiver and a PC with the service center configuration (SCC) software, USB Transceiver mode enables settings configuration and information download directly between the TripSaver II recloser and the SCC software loaded on a PC.

Exclusive use of one radio mode at a time is required. The mode is selected by applying the side magnet, cordless power module, and line current in combinations as shown in Table 6 on page 86. Radio activation is different for firmware versions 1.7 and 1.8 and later, so methods for both versions are included in Table 6 on page 86.

### DANGER

The TripSaver II Cutout-Mounted Recloser **MUST** be de-energized and removed from the utility pole before attaching the “corded” power module (power module with ac adapter and extension cord) to the base of the TripSaver II recloser. The corded power module is **ONLY** intended to be used for setup and data collection when the TripSaver II recloser is de-energized and removed from the utility pole. Failure to remove the recloser from the pole before attaching the “corded” power module can cause arcing, burns, electric shock, and death.

### **Cybersecurity—Communications Gateway Radio Mode**

The TripSaver II recloser and TripSaver II Communications Gateway use open standards such as IPv6 and 802.15.4 MAC and PHY layers as a foundation for communication security.

When a TripSaver II Communications Gateway is commissioned for the first time, it generates a completely random network master key. The network master key is, therefore, unique per TripSaver II Communications Gateway and the paired TripSaver II reclosers, allowing communications only between these devices. The network master key is used to authenticate access and to derive the encryption keys for data encryption.

The TripSaver II recloser upon power up will identify itself to the communications gateway and use a secure algorithm to establish an authenticated and encrypted connection to the gateway. The operator of the gateway must then explicitly add the TripSaver II recloser to the local network via the secure web user interface.

Communications between the TripSaver II recloser and the communications gateway for operational/application data are always encrypted using AES with a 128-bit encryption key derived using a one-way secure hashing function that combines the network master key learned during the pairing, with the key sequence numbers, which are automatically changed on a periodic basis.

**Table 6. Radio Mode**

Gateway Mode Configuration Setting: Enabled or Disabled?	Line Power Available?	Cordless Power Module Available? <sup>①</sup>	Side Magnet Applied?	Side Magnet Configuration Setting: Is Enabled?	Radio Mode (Firmware v1.7)	Radio Mode (Firmware v1.8 and later)
Disabled	Yes	No	No	●	Radio off	Radio off
Disabled	●	Yes	No	●	USB transceiver	USB transceiver
Disabled	Yes	No	Yes	No	Radio off	Radio off
Disabled	Yes	No	Yes	Yes	USB transceiver	USB transceiver
Disabled	●	Yes	Yes	No	USB transceiver	USB transceiver
Enabled	Yes	No	No	●	Communications gateway	Communications gateway
Enabled	●	Yes	No	●	USB transceiver	USB transceiver
Enabled	Yes	No	Yes	No	Communications gateway	Communications gateway
Enabled	Yes	No	Yes	Yes	Communications gateway	Communications gateway
Enabled	●	Yes	Yes	No	USB transceiver	Communications gateway

① The corded ac power module should never be connected to the TripSaver II recloser when the recloser is powered by line current. See the Danger message on page 85.

● This could be set to "Yes" or "No" without affecting the Radio mode.



## Gateway Controller Module Indicator Lights

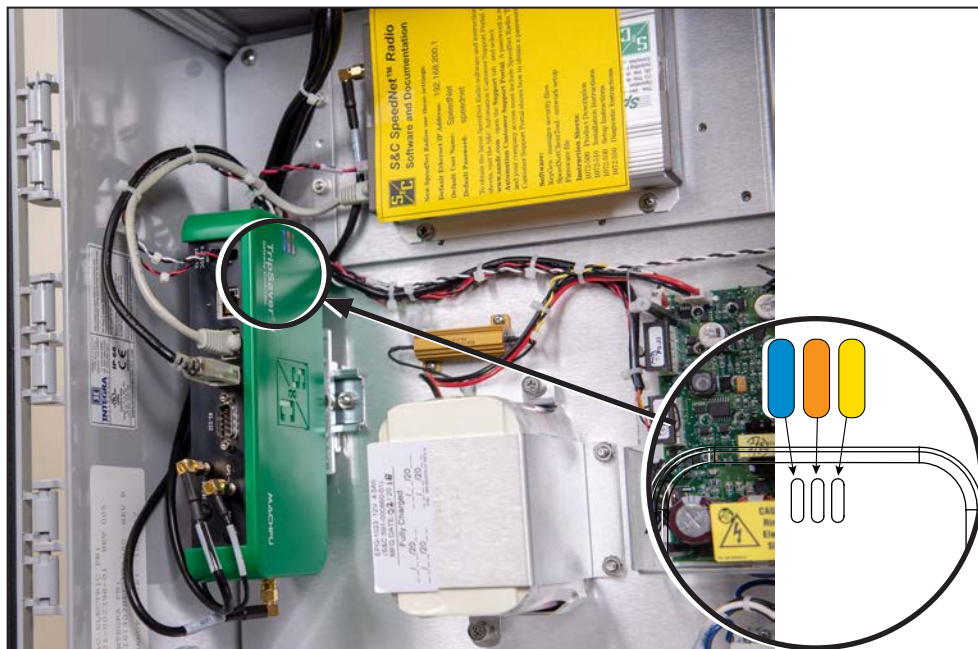


Figure 77. LED indicator lights.

**Blue LED:** The gateway controller module is connected to power.

**Orange LED:** This is the “Heartbeat LED.” This LED indicates various stages during the module’s **Startup** sequence. When the module is first powered on, the orange LED will be off for 15 seconds and then on for 10 seconds. When the module starts initializing, the orange LED will blink rapidly for 2 seconds (8 blinks) and then stay off for 3 seconds. When initialization is complete, it blinks for 4 seconds (4 blinks) and stays off for 1 second.

**Yellow LED:** Always On. Reserved for future use.

### Regulatory Information

This document contains statements that are required for compliance with the rules and policies of various national and international regulatory agencies. The information is current as of the date of this publication but may be subject to change without notice. For the most recent version of this Instruction Manual with the most up to date regulatory information, visit [sandc.com](http://sandc.com).

#### **United States of America–FCC (Federal Communication Commission)**

This device complies with part 15 of the FCC rules and regulations regarding unlicensed transmissions. Operation is subject to the following two conditions: (1) This device may not cause harmful interference and (2) this device must accept any interference.

**IMPORTANT!** Changes or modifications not expressly approved by S&C Electric Company 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 A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

#### **Canada–ISED (Innovation, Science & Economic Development Canada)**

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.

*Cet appareil est conforme aux normes Industry Canada exemptes de licence RSS standard(s). Son fonctionnement est soumis aux deux conditions suivantes: (1) cet appareil ne doit pas provoquer d'interférences et (2) cet appareil doit accepter toute interférence, y compris les interférences susceptibles de provoquer un fonctionnement indésirable.*

The changes or modifications not expressly approved by the S&C Electric Company could void the user's authority to operate the equipment.

#### **CAN ICES-3 (A)/NMB-3(A)**

##### **Australia/New Zealand (ACMA)**

*The above-mentioned product complies with the requirements of the relevant ACMA Standards made under the Radiocommunications Act 1992 and the Telecommunications Act 1997. These Standards are referenced in notices made under section 182 of the Radiocommunications Act and 407 of the Telecommunications Act.*

**Brazil (ANATEL):**

*Atendimento à Regulamentação Anatel*

Este equipamento não tem direito à proteção contra interferência prejudicial e não pode causar interferência em sistemas devidamente autorizados.

Este produto está homologado pela ANATEL, de acordo com os procedimentos regulamentados pela Resolução 242/2000, e atende aos requisitos técnicos aplicados.

Para maiores informações, consulte o site da ANATEL. **[www.anatel.gov.br](http://www.anatel.gov.br)**

