# Table of Contents

## Section Page

### Introduction
- Qualified Persons ......................... 2
- Read this Instruction Sheet .................. 2
- Retain this Instruction Sheet .................. 2
- Proper Application .......................... 2
- Warranty .................................. 2

### Safety Information
- Understanding Safety-Alert Messages .......... 3
- Following Safety Instructions .................... 3
- Replacement Instructions and Labels ............ 3

### Safety Precautions ........................ 4

### Shipping and Handling
- Packing ................................... 5
- Inspection .................................. 5
- Handling ................................... 5
- Storage .................................... 5
- Returning .................................. 5

### Mounting, Powering Up, and Securing the Communications Gateway ................. 6
- Mounting the Communications Gateway to a Pole .................. 7
- Powering Up the Communications Gateway ................... 8
- Securing the Communications Gateway .......... 8

### Installing and Replacing a Radio
- Installing a New Radio ....................... 9
- Replacing a Radio .......................... 10

### Installing and Replacing a Backup Battery
- Installing a New Battery ..................... 11
- Replacing a Battery ........................ 12

### Installing Remote Antenna Kits
- Installing Remote Antenna .................. 13
- Kit 903-002702-02/01 ...................... 13
- Kit 903-002701-01/02 ...................... 14
- Kit 903-002700-02/03 ...................... 14

### Installing and Replacing a Local Antenna
- Installing Local Antenna 904-002450-02 ........ 15
- Replacing a Local Antenna .................. 15

### Configuring the Communications Gateway
- Software User’s Guide ....................... 16
- General Status ............................. 19
- Gateway Settings ............................ 19
- Device Management .......................... 33
- TripSaver® II Service Center
  - Configuration Software ..................... 34
- Remote Drop Open .......................... 36
- Gang/Local Operation ....................... 39
- DNP3 Master Settings ....................... 42
- DNP3 Outstation Settings .................... 44
- User Roles ................................ 51
- Security Settings ............................ 52
- Enabling Remote Web Access .................. 54
- Profile ................................... 56
- Diagnostics ................................. 56

### Commissioning (Pairing) a TripSaver® II Recloser for Use with the Communications Gateway
- Service Center Pairing a TripSaver II Recloser with Firmware Version 1.8 ........... 58
- Field Pairing a TripSaver II Recloser with Firmware Version 1.6 or 1.7 Installed on the Utility Pole and Powered by Line Current ..................... 59
- Troubleshooting .............................. 59

### Quick Installation Checklist
- Interface Pinouts ........................... 62
- Power System Diagram ...................... 63

### Appendix A
- Interface Pinouts ........................... 62
- Power System Diagram ...................... 63
Introduction

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 your TripSaver II Communications via Gateway system. The latest version is available online in PDF format at sandc.com/en/support/product-literature. Familiarize yourself with Safety Information and Safety Precautions on pages 3 and 4.

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 you can easily retrieve and refer to it.

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.

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.
Several types of safety-alert messages may appear throughout this instruction sheet and on labels attached to crate, packing, and equipment. Familiarize yourself 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 you do not understand any portion of this instruction sheet and need assistance, contact your nearest S&C Sales Office or S&C Authorized Distributor. Their telephone numbers are listed on S&C’s website 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 your TripSaver II Communications via Gateway system.

**Replacement Instructions and Labels**

If additional copies of this instruction sheet are needed, contact your nearest S&C Sales Office, S&C Authorized Distributor, or S&C Headquarters. You can also download this instruction sheet from S&C’s website 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 your nearest S&C Sales Office, S&C Authorized Distributor, or S&C Headquarters.
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 box to the pole
- 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

<table>
<thead>
<tr>
<th>NOTICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>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 20 lbs. (9 kg); follow proper lifting techniques to avoid injury.</td>
</tr>
</tbody>
</table>

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 Distributer, or S&C Headquarters.
Mounting, Powering Up, and Securing the Communications Gateway

Figure 1. The TripSaver II Communications Gateway.
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 gateway should be mounted no further than 100 feet (30.5 m) below TripSaver II Cutout-Mounted Reclosers, ideally no more than 30 feet (9.1 m) away from the communications gateway and in direct line of sight. If conditions and utility practice permit, mounting out of public reach is recommended to deter vandalism. The communications gateway enclosure has a door-alarm provision for security.
Follow these steps to power up 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.** Open the box.

**STEP 3.** Run the ac power cable down the pole. The unterminated end of the cable should be connected to the overhead transformer.

**STEP 4.** 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 7.

**STEP 5.** After a short delay, LEDs on the power supply/control I/O (PSIO) board and the gateway controller should light up, indicating the communications gateway is receiving power. See Figure 1 on page 6 and Figure 3.

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 7.

**STEP 2.** The door latches accept locks with a maximum shackle diameter of 3/8-inches (9.5 mm).
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.
Installing and Replacing 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 13 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 8/32-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 9.

STEP 2. Remove the existing field-area network radio. See Figure 4 on page 9.
(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.


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 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 12.

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.

**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.](image)

(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 cap 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 power supply/control I/O (PSIO) board. The acrylic safety cover over the PSIO board does not need to be removed to make this connection.
STEP 4. Replace the ac-line fuse located at the lower right corner of the gateway box and leave the ac cable connector disconnected.

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

STEP 6. Reconnect the ac-cable connector.

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 7) and then disconnect the ac-line fuse located at the lower right corner of the gateway box. See Figure 5 on page 11.

STEP 2. Remove the pre-installed battery located in the bottom-middle section of the enclosure. See Figure 6.
   (a) Disconnect the red and black battery leads from white 2-pin connector on the PSIO board. See Figure 5 on page 11.
   (b) Unscrew the four cap nuts that hold the battery pack and top bracket in place.
   (c) 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 previous section: “Installing a New Battery” section on page 11.
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. 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.
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. 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. 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 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.”
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 9. 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.

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 on page 17.
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.

**Note:** Because the end user can change the IP address range, or even disable DHCP completely and change the gateway to a static IP, it is important to make a note of any IP settings changes. When relocating or setting up a 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 on page 18.

**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/.
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 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-upper case and one lower-case character. Numbers and special characters are also allowed but not required. <Space>, <Tab>, <&> characters are not allowed.

---

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 19.
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 will be permissible 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,” and “Gateway Hardware” 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. See Figure 13.

![Figure 13. The General Status screen.](image)

Gateway Settings

The Gateway Settings screen contains the “Gateway Name,” “Ethernet 1 (LAN),” “Ethernet 2 (WAN),” “Gateway Configuration,” “Firmware Upgrade,” and “Reboot Gateway” 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 on page 20.
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 the **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.

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.](image)

**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 the user uses serial back-haul networks or does not have a WAN, this panel will not require entries.

![Figure 17. The Ethernet 2 (WAN) fields.](image)
Configuring the Communications Gateway

**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).

**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.

![Gateway Settings](image)

**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.

**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 dialogue boxes allowing navigation on a PC to a configuration file for “Import” or the saving of a file for “Export.” See Figure 19 on page 23.
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 24.
## Configuring the Communications Gateway

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Data Type of Value</th>
<th>Range of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Type of interface used for DNP3. See DNP3 Interface on DNP3 Master Settings page.</td>
<td>String</td>
<td>TCP, UDP, Serial</td>
</tr>
<tr>
<td>serialBaud</td>
<td>Serial baud rate, used if interface=Serial. See Baud Rate on DNP3 Master Settings page.</td>
<td>Integer</td>
<td>9600, 19200, 38400, 57600, 115200</td>
</tr>
<tr>
<td>serialStopBits</td>
<td>Serial stop bits, used if interface=Serial. See Stop Bits on DNP3 Master Settings page.</td>
<td>Integer</td>
<td>1 or 2</td>
</tr>
<tr>
<td>serialParity</td>
<td>Serial parity, used if interface=Serial. See Parity on DNP3 Master Settings page.</td>
<td>String</td>
<td>None, odd, even</td>
</tr>
<tr>
<td>serialFlow</td>
<td>Serial flow control, used if interface=Serial. See Flow Control on DNP3 Master Settings page.</td>
<td>String</td>
<td>None, RTS/CTS, XON/XOFF</td>
</tr>
<tr>
<td>addressMode</td>
<td>DNP3 addressing mode. See Addressing Type on DNP3 Outstation Settings page.</td>
<td>String</td>
<td>Concentrator</td>
</tr>
<tr>
<td>gatewayAddress</td>
<td>DNP3 address of gateway. See Gateway DNP3 Address on DNP3 Outstation Settings page.</td>
<td>Integer</td>
<td>1 … 65,519</td>
</tr>
<tr>
<td>tcpKeepAlive</td>
<td>See description for TCP Keepalive Timer on DNP3 Outstations Settings page.</td>
<td>Integer</td>
<td>Any integer value</td>
</tr>
<tr>
<td>unsolicitedIndefiniteRetries</td>
<td>See description for Unsolicited Responses Retried Indefinitely on DNP3 Outstations Settings page.</td>
<td>Boolean</td>
<td>0 (FALSE), 1 (TRUE)</td>
</tr>
<tr>
<td>unsolicitedResponsesToConfirm</td>
<td>See description for Number of Retries for Confirm on DNP3 Outstations Settings page.</td>
<td>Integer</td>
<td>Any integer value</td>
</tr>
<tr>
<td>unsolicitedResponsesDelay</td>
<td>See description for Delay Before Retries on DNP3 Outstations Settings page.</td>
<td>Integer</td>
<td>1 … 300</td>
</tr>
<tr>
<td>disableObjectFlagCommLost</td>
<td>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.</td>
<td>Boolean</td>
<td>True or False</td>
</tr>
<tr>
<td>dnp3InactivityTimerDuration</td>
<td>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.</td>
<td>Integer</td>
<td>0 - 1500</td>
</tr>
<tr>
<td>devicename</td>
<td>User-specified device name, to be reported via DNP3 in group 0, attribute 247. See Gateway Name on Gateway Settings page.</td>
<td>String</td>
<td>n/a</td>
</tr>
<tr>
<td>gangOperationEnabled</td>
<td>This setting disables the Gang Operation feature in the gateway, independent of the individual settings for the TripSaver II recloser. When set to true, the Gang Operation feature is enabled and will operate according to the settings defined on the Gang/Local tab for each TripSaver II recloser. When set to false the Gang Operation feature will not operate.</td>
<td>Boolean</td>
<td>True or False</td>
</tr>
<tr>
<td>gangOperationMaxRetries</td>
<td>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.</td>
<td>Integer</td>
<td>0 - 2592000</td>
</tr>
<tr>
<td>gangOperationRetryTime</td>
<td>The time interval between gang operation retry attempts in seconds.</td>
<td>Integer</td>
<td>1 - 3600</td>
</tr>
<tr>
<td>unsolRespDelayEventCount</td>
<td>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.</td>
<td>Integer</td>
<td>1 - 60</td>
</tr>
<tr>
<td>unsolRespDelayTime</td>
<td>The maximum amount of time the gateway will queue DNP3 unsolicited events before sending to the SCADA master, in units of milliseconds.</td>
<td>Integer</td>
<td>100 - 120000</td>
</tr>
<tr>
<td>enableSingleUnitOperation</td>
<td>This setting enables or disables the single-unit Drop Open feature in the gateway, independent of the individual settings for the TripSaver II recloser. When set to true, the single-unit Local Drop Open feature is enabled and will operate according to the settings defined on the Gang/Local tab for each TripSaver II recloser. When set to false, the Single Unit Operation feature will not operate.</td>
<td>Binary</td>
<td>True or False</td>
</tr>
<tr>
<td>remoteDropOpenEnabled</td>
<td>This setting enables or disables the Remote Drop Open feature in the gateway, independent of the individual settings for the TripSaver II recloser. When set to true, the Remote Drop Open feature is enabled and will operate according to the settings defined on the Gang/Local tab for each TripSaver II recloser. When set to false, the Remote Drop Open feature will not operate.</td>
<td>Binary</td>
<td>True or False</td>
</tr>
</tbody>
</table>
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:

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

The configuration settings that can be specified in this section of the document are described in Table 2 on page 26.
# Configuring the Communications Gateway

## Table 2. Import and Export Settings Configuration

<table>
<thead>
<tr>
<th>Parameter Group</th>
<th>Attribute</th>
<th>Description</th>
<th>Data Type</th>
<th>Range of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;DNP3Masters&gt;</code></td>
<td>unsolicitedenabled</td>
<td>Boolean indicating whether the gateway will attempt to send DNP3 unsolicited responses to the SCADA master. See Unsolicited Response on DNP3 Master Settings page.</td>
<td>Boolean</td>
<td>True or False</td>
</tr>
<tr>
<td></td>
<td>port</td>
<td>Gateway’s TCP or UDP listen port for receiving IP packets from the SCADA master.</td>
<td>Integer</td>
<td>1024 … 49,151</td>
</tr>
<tr>
<td></td>
<td>ipaddress</td>
<td>SCADA master’s IP address. Currently ignored by the gateway as it will accept traffic from any IP address. See IPv4 Address on DNP3 Master Settings page.</td>
<td>IP address (dotted decimal)</td>
<td>Any valid IP address</td>
</tr>
<tr>
<td></td>
<td>dnp3address</td>
<td>SCADA master’s DNP3 address. See DNP3 Address on DNP3 Master Settings page.</td>
<td>Integer</td>
<td>1 … 65,519</td>
</tr>
<tr>
<td><code>&lt;BinaryInputSetPoints&gt;</code></td>
<td>statuspoint</td>
<td>See Status Point on DNP3 Outstation Settings page.</td>
<td>Integer</td>
<td>0 … 147</td>
</tr>
<tr>
<td><code>&lt;BinaryInputSetPoints&gt;</code></td>
<td>codedescription</td>
<td>See Code Description on DNP3 Outstation Settings page.</td>
<td>Integer</td>
<td>Per S&amp;C Instruction Sheet 461-560</td>
</tr>
<tr>
<td><code>&lt;BinaryInputSetPoints&gt;</code></td>
<td>eventclass</td>
<td>See Class on DNP3 Outstation Settings page. A value of 0 corresponds to NO EVENT.</td>
<td>Integer</td>
<td>0,1,2,3</td>
</tr>
<tr>
<td><code>&lt;AnalogInputSetPoints&gt;</code></td>
<td>statuspoint</td>
<td>See Status Point on DNP3 Outstation Settings page.</td>
<td>Integer</td>
<td>0…20</td>
</tr>
<tr>
<td><code>&lt;AnalogInputSetPoints&gt;</code></td>
<td>codedescription</td>
<td>See Code Description on DNP3 Outstation Settings page.</td>
<td>Integer</td>
<td>Per S&amp;C Instruction Sheet 461-560</td>
</tr>
<tr>
<td><code>&lt;AnalogInputSetPoints&gt;</code></td>
<td>eventclass</td>
<td>See Class on DNP3 Outstation Settings page. A value of 0 corresponds to NO EVENT.</td>
<td>Integer</td>
<td>0,1,2,3</td>
</tr>
<tr>
<td><code>&lt;BinaryOutputSetPoints&gt;</code></td>
<td>statuspoint</td>
<td>See Status Point on DNP3 Outstation Settings page.</td>
<td>Integer</td>
<td>0 … 8</td>
</tr>
<tr>
<td><code>&lt;BinaryOutputSetPoints&gt;</code></td>
<td>codedescription</td>
<td>See Code Description on DNP3 Outstation Settings page.</td>
<td>Integer</td>
<td>Per S&amp;C Instruction Sheet 461-560</td>
</tr>
<tr>
<td><code>&lt;BinaryOutputSetPoints&gt;</code></td>
<td>eventclass</td>
<td>See Class on DNP3 Outstation Settings page. A value of 0 corresponds to NO EVENT.</td>
<td>Integer</td>
<td>0,1,2,3</td>
</tr>
<tr>
<td><code>&lt;BinaryOutputSetPoints&gt;</code></td>
<td>fixeddeadband</td>
<td>See Fixed Deadband on DNP3 Outstation Settings page. Set to ‘disabled’ to disable fixed deadband reporting for this setpoint.</td>
<td>Integer or &quot;disabled&quot;</td>
<td>Any non-negative integer value or &quot;disabled&quot;</td>
</tr>
<tr>
<td><code>&lt;BinaryOutputSetPoints&gt;</code></td>
<td>percentdeadband</td>
<td>See Pct Deadband on DNP3 Outstation Settings page. Set to “disabled” to disable percent deadband reporting for this setpoint.</td>
<td>Integer or &quot;disabled&quot;</td>
<td>Any non-negative integer value or &quot;disabled&quot;</td>
</tr>
<tr>
<td><code>&lt;BinaryOutputSetPoints&gt;</code></td>
<td>scaling</td>
<td>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 DNP3 Outstation Settings page.</td>
<td>float</td>
<td>0.001 … 1000</td>
</tr>
<tr>
<td><code>&lt;CounterSetPoints&gt;</code></td>
<td>statuspoint</td>
<td>See Status Point on DNP3 Outstation Settings page.</td>
<td>Integer</td>
<td>0 … 19</td>
</tr>
<tr>
<td><code>&lt;CounterSetPoints&gt;</code></td>
<td>codedescription</td>
<td>See Code Description on DNP3 Outstation Settings page.</td>
<td>Integer</td>
<td>Per S&amp;C Instruction Sheet 461-560</td>
</tr>
<tr>
<td><code>&lt;CounterSetPoints&gt;</code></td>
<td>eventclass</td>
<td>See Class on DNP3 Outstation Settings page. A value of 0 corresponds to NO EVENT.</td>
<td>Integer</td>
<td>0,1,2,3</td>
</tr>
<tr>
<td><code>&lt;CounterSetPoints&gt;</code></td>
<td>fixeddeadband</td>
<td>See Fixed Deadband on DNP3 Outstation Settings page. Set to “disabled” to disable fixed deadband reporting for this setpoint.</td>
<td>Integer or &quot;disabled&quot;</td>
<td>Any non-negative integer value or &quot;disabled&quot;</td>
</tr>
<tr>
<td><code>&lt;CounterSetPoints&gt;</code></td>
<td>percentdeadband</td>
<td>See Pct Deadband on DNP3 Outstation Settings page. Set to “disabled” to disable percent deadband reporting for this setpoint.</td>
<td>Integer or &quot;disabled&quot;</td>
<td>Any non-negative integer value or &quot;disabled&quot;</td>
</tr>
<tr>
<td><code>&lt;BinaryOutputSetPoints&gt;</code></td>
<td>Retry Behavior</td>
<td>Will either discard the retry attempt or retry for the set interval and number of attempts.</td>
<td>Binary</td>
<td>Discard or Queue</td>
</tr>
<tr>
<td><code>&lt;BinaryOutputSetPoints&gt;</code></td>
<td>Retry Interval</td>
<td>Time, in seconds, between retry attempts.</td>
<td>Integer</td>
<td>1 to 3600</td>
</tr>
<tr>
<td><code>&lt;BinaryOutputSetPoints&gt;</code></td>
<td>Max Retry Attempts</td>
<td>The maximum number of times the output will be retried</td>
<td>Integer</td>
<td>1 to 2,592,000</td>
</tr>
</tbody>
</table>
Import Configuration
Follow these steps to complete the Import Configuration function. See Figures 20 and 21.

STEP 1. Under the Gateway Configuration panel, click on the Import Configuration button. A Web User Interface (WUI) dialogue box opens.

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 dialogue box.

STEP 5. Click on the Import button.

STEP 6. Click on the Save button.
Configuring the Communications Gateway

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

STEP 1. On the Gateway Configuration panel, click on the Export Configuration button. A WUI dialogue box opens 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 22. The Export Configuration dialogue box.

Figure 23. Export File Save navigation.
Firmware Upgrade

This panel enables the loading of firmware versions onto the communications gateway. See Figure 24.

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/.

**STEP 2.** Click on the **Upload Firmware File** button on the Firmware Upgrade panel. See Figure 24.

**STEP 3.** A Windows dialogue box will open. See Figure 25. Navigate to the firmware file and select it. Click on the **Open** button.
STEP 4. The file loads to the communications gateway. After the upload completes, the gateway will confirm that the upload was successful. See Figures 26 and 27.

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 28.
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 29.

Figure 29. The dialog box showing the firmware-verification process is complete.

STEP 7. Click on the Upgrade button. This will start the upgrade process. See Figures 30 and 31.

Figure 30. Start the firmware upgrade process by clicking on the Upgrade button.

Figure 31. The firmware-upgrade process progress bar.
STEP 8. When the gateway has completed processing the upgrade, it will display a notification. See Figure 32. 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 page after the reboot completes. See Figure 11 on page 18. Log in and confirm the new firmware has been installed successfully by going to the General Status screen.

Reboot Gateway

The red colored Reboot button enables the user to restart the communications gateway. When selected, a dialogue box opens for confirmation of 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 33.
Device Management

The purpose of the **Device Management** menu 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 window.

**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 58 for a walk-through of the pairing process.

To add a TripSaver II recloser, click on the **Add TripSaver II** button on the top right of the page. A pop-up dialogue box will open. Enter the recloser's Transceiver ID and the desired device name. See Figure 34 and Figure 35 on page 34. 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 page 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 58.

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

![Figure 34. Pairing of a TripSaver II recloser with the communications gateway.](image-url)
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 the 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.

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 on the 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. See Figure 36.

![Enable Service Center Configuration toggle button](image1)

**Figure 36. The Enable Service Center Configuration toggle button.**

When the **Service Center Configuration** mode is enabled, the dialogue box opens. See Figure 37.

![Enable Service Center Configuration pop-up](image2)

**Figure 37. 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 38 on page 36.

---

**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.
Remote Drop Open

TripSaver II reclosers supplied with the 30-second option (-O), firmware version 1.8, 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 44 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 say “Yes.” See Figure 39 on page 37.
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 39. Enabling the Remote Drop Open feature in the communications gateway.](image)

**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 40.

![Figure 40. Activating the Remote Drop Open feature in the TripSaver II recloser and the communications gateway.](image)
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 41.

**Figure 41. 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 42.

**Figure 42. A TripSaver II recloser when the Remote Drop Open feature is not factory-enabled in the recloser.**
Local Drop Open Operation Settings

TripSaver II reclosers supplied with firmware versions 1.7 and 1.8 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 43.

![Figure 43. The communications gateway requires a backup battery for Local/Gang operation.](image)

New to TripSaver II Communications Gateway firmware version 3.0 and only available with TripSaver II recloser firmware version 1.8 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 44.

![Figure 44. Enabling the single-unit Local Drop Open operation.](image)
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.

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 45.

Two other features that should be configured are the **Local Drop Open Retry Time** and the **Local Drop Open Max Retries**. See Figure 46.
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 of 0-3600 seconds). The default time is 10 seconds.

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

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 equipment damage and 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 47.

![Figure 47. Performing a Gang Trip operation.](image-url)
A TripSaver II recloser and paired communications gateway can be configured for both **Single Unit Operation** and **Gang Operation** functions. See Figure 48.

**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 49.

**Figure 48. A Single Unit and Gang operation.**

**Figure 49. 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 selection 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 50.

**Figure 50. 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 dialogue 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 51.

**Figure 51. The DNP3 Master with serial configuration panel.**
The purpose of the **DNP3 Outstation Settings** menu 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 3.0, 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 52.

![Figure 52. The DNP3 Addressing panel.](image)

### 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 53

![Figure 53. The DNP3 Outstation General Settings panel.](image)
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 54.

![Figure 54. The Unsolicited Response panel.](image)

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 55.

![Figure 55. The Status (Binary Input) point entry field.](image)

**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 dialogue box will appear with code definitions for all TripSaver II reclosers paired with the communications gateway. See Figure 56 on page 47. 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 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 57 shows an example of Status Point 1 after being saved to the communications gateway.
**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 58.

![Figure 58. The Analog Input Points configuration screen.](image)

**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 dialogue 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 59.

Figure 59. 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 dialogue 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 60. Mapping these points will make them available in SCADA.

Figure 60. 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 dialogue 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 dialogue box will open with the required User, Password, and Confirm Password fields, and a drop-down box to select user type. See Figure 61.

![Figure 61. The User Role configuration screen.](image)

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

<table>
<thead>
<tr>
<th>Table 3. User Role Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Page</strong></td>
</tr>
<tr>
<td>General Status</td>
</tr>
<tr>
<td>Gateway Settings</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Device Management</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Remote Drop Open</td>
</tr>
<tr>
<td>Gang/Local Operation</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>TripSaver II Service Center Configuration Software</td>
</tr>
<tr>
<td>DNP3 Master Settings</td>
</tr>
<tr>
<td>DNP3 Outstation Settings</td>
</tr>
<tr>
<td>User Roles</td>
</tr>
<tr>
<td>Security Settings</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Profile</td>
</tr>
<tr>
<td>Diagnostics</td>
</tr>
</tbody>
</table>
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 62. Enabling a secure tunnel from the communications gateway creates an authenticated, encrypted, and integrity-protected path through which DNP3 traffic will pass.

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 OpenVPN option from the drop-down menu. A dialogue box will open for field entry. When the fields are completed, click on the Add button to complete and add the tunnel profile. See Figure 62.

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 OpenVPN option from the drop-down menu. A configuration dialogue box will open. See Figure 63.
Follow these steps to add OpenVPN:

**STEP 1.** Enter the IP (private) address of the VPN server in the IPsec Server IP box.

**STEP 2.** Enter the Server port number into the Server Port box.

**STEP 3.** Enter the (private) IP address into the Server Tunnel IP box.

**STEP 4.** Select either UDP or TCP transport protocol into the Transport Protocol box.

**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 box.

**STEP 8.** Choose a selection from the TLS Security drop-down menu.

**STEP 9.** Enter a key in the TLS Crypt Key box.

**STEP 10.** Enter the CA certificate into the CA Certificate box.

**STEP 11.** Enter the device certificate into the Device Certificate box.

**STEP 12.** Enter the device private key into the Device Private Key box.

**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 DNP3 binary output setpoint, which must also be enabled to allow this traffic. See Figure 64. See the “Enabling Remote Web Access” section on page 54.

**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`.

![Security Settings](image)
Configuring the Communications Gateway

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.** In the Profile tab, 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 65.

![Figure 65. The Remote Web Access slide selector.](image)

**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 66.

![Figure 66. Configuring the Remote Web UI DNP3 command (binary output).](image)
STEP 4. See Figure 67. 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”

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 59:

- 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.

- 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.
Configuring the Communications Gateway

Profile

The Profile menu enables the present user logged in to the communication gateway to change his or her password credentials. See Figure 68.

![Profile screen](image)

**Figure 68. The Profile screen.**

Diagnostics

The purpose of the Diagnostics screen is to initiate the retrieval of the Diagnostic and Event Log files. See Figure 69.

![Diagnostics screen](image)

**Figure 69. The Diagnostics screen retrieves files.**
When any of the Retrieve buttons is selected, a dialogue box opens notifying the user of the file-retrieval interval. See Figure 70.

Figure 70. The Diagnostic Log retrieval interval dialogue 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 71.

Figure 71. The Diagnostic Log completion dialogue box.
Service Center Pairing a TripSaver II Recloser with Firmware Version 1.8

<table>
<thead>
<tr>
<th>DANGER</th>
</tr>
</thead>
<tbody>
<tr>
<td>The TripSaver II Cutout-Mounted Recloser MUST be de-energized and removed from the utility pole before attaching the &quot;corded&quot; 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.</td>
</tr>
</tbody>
</table>

With the introduction of TripSaver II Cutout-Mounted Recloser firmware version 1.8, 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 v1.8, 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 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 16. 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 that 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 page 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 59.

**STEP 4.** When paired, disconnect the magnet tool’s magnet and 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.
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 details on the 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 1.8, 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 version 1.8 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.

**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 16. 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 that 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” page 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.

**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. 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.

**Troubleshooting**

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. 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 menu and select the Communications Mode drop-down box. 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 16. 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.
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
  • 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 up

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).
The RS-232 port of the gateway controller module (green box) is configured as data-terminal equipment. See Table 3.

### Table 3. Gateway Controller Module RS-232 Interface Pinout

<table>
<thead>
<tr>
<th>Pin</th>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>NC</td>
<td>No Connection</td>
</tr>
<tr>
<td>2</td>
<td>RX from Radio</td>
<td>RS-232 Receive</td>
</tr>
<tr>
<td>3</td>
<td>TX to Radio</td>
<td>RS-232 Transmit</td>
</tr>
<tr>
<td>4</td>
<td>NC</td>
<td>No Connection</td>
</tr>
<tr>
<td>5</td>
<td>TX to Radio GND</td>
<td>Signal Ground</td>
</tr>
<tr>
<td>6</td>
<td>NC</td>
<td>No Connection</td>
</tr>
<tr>
<td>7</td>
<td>RTS to Radio</td>
<td>Request to Send</td>
</tr>
<tr>
<td>8</td>
<td>CTS to Radio</td>
<td>Clear to Send</td>
</tr>
<tr>
<td>9</td>
<td>NC</td>
<td>No Connection</td>
</tr>
</tbody>
</table>

Ethernet Ports 1 and 2 use RJ-45 connectors with the pinout shown in Table 4. 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 4. Ethernet Ports

<table>
<thead>
<tr>
<th>Pin</th>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TXD+</td>
<td>Transmit</td>
</tr>
<tr>
<td>2</td>
<td>TXD-</td>
<td>Transmit</td>
</tr>
<tr>
<td>3</td>
<td>RXD+</td>
<td>Receive</td>
</tr>
<tr>
<td>4</td>
<td>NC</td>
<td>No Connection</td>
</tr>
<tr>
<td>5</td>
<td>NC</td>
<td>No Connection</td>
</tr>
<tr>
<td>6</td>
<td>RXD-</td>
<td>Receive</td>
</tr>
<tr>
<td>7</td>
<td>NC</td>
<td>No Connection</td>
</tr>
<tr>
<td>8</td>
<td>NC</td>
<td>No Connection</td>
</tr>
</tbody>
</table>
Figure 72. The communications gateway power system diagram.