Installation, Operation, and Configuration

Table of Contents

Introduction	2
Qualified Persons	2
Read this Instruction Sheet	2
Retain this Instruction Sheet.	2
Proper Application	2
warranty	3
Safety Information.	4
Understanding Safety-Alert Messages.	4
Pollowing Safety Instructions	4 1
Location of Safety Labels	4
Cofety Presentions	
Salely Precautions	
Shipping and Handling	7
	7
	/
Storage	/
Returning	7
Mounting Powering and Securing the	
Communications Gateway	8
Mounting the Communications Gateway to a Pole.	9
Powering the Communications Gateway	10
Securing the Communications Gateway	10
Installing and Replacing a Radio	. 11
Installing a New Radio	11
Replacing a Radio	12
Installing and Replacing a Backup Battery	. 13
Installing a New Battery	13
Replacing a Battery	14
Installing Remote Antenna Kits	. 15
Installing Remote Antenna Kit 903-002702-02/01.	15
Installing Remote Antenna Kit 903-002701-01/02 .	16
Installing Remote Antenna Kit 903-002700-02/03.	17
Installing and Replacing a Local Antenna	. 18
Installing Local Antenna 904-002450-02	18
Replacing a Local Antenna.	18

Configuring the Communications Gateway	19
Software User's Guide	19
Protocol in the Communications Gateway	23
General Status	24
Gateway Settings	25
Device Management	45
TripSaver® II Service Center Configuration Software	46
Remote Drop Open.	48
Gang/Local Operation	51
IFC 104 Setnoints	57
IEC104 Controlling Station	62
IEC104 Controlled Station	63
Security Settings	64
Profile	68
Diagnostics	68
Commissioning (Pairing) a TripSaver II	
Recolser for Use with the Communications	
Gateway	71
with Firmware Version 1.8 or Later.	71
Field-Pairing a TripSaver II Recloser with	
Firmware Version 1.6 or 1.7 Installed on the	
Utility Pole and Powered by Line Current	72
Troubleshooting	74
Signal Interference	74
Pairing Process Takes Longer Than Expected	74
Quick Installation Checklist	75
Appendix A	76
Interface Pinouts	76
Power System Diagram	77
Understanding the Radio Mode	77
Gateway Controller Module Indicator Lights	79
Appendix B	80
Regulatory Information	80
United States of America–FCC (Federal	00
Connunication Commission)	00
Development Canada)	80
CAN ICES-3 (A)/NMB-3(A)	81
Australia/New Zealand (ACMA)	81
Brazil (ANATEL):	81



Introduction

Qualified	
Persons	
	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	NOTICE
Sheet	Thoroughly and carefully read this instruction sheet and all materials included in the product's instruction handbook before installing or operating the TripSaver II Communications via Gateway system. Become familiar with the Safety Information "Several types of safety-alert messages may appear throughout this instruction sheet and on labels and tags attached to the TripSaver II Communications Gateway. Become familiar with the Safety Information on page 4 and Safety Precautions on page 6. The latest version of this publication is available online in PDF format at https://www.sandc.com/en/contact-us/product-literature/.
Retain this Instruction Sheet	This instruction sheet is a permanent part of the TripSaver II Communications via Gateway system. Designate a location where users can easily retrieve and refer to this publication.
Proper	
Application	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 system are listed in the ratings table in Specification Bulletin 461-33. The ratings are also on the nameplate affixed to the product.

Warranty

The warranty and/or obligations described in S&C's Price Sheet 150, "Standard Conditions of Sale-Immediate Purchasers in the United States," (or Price Sheet 153, "Standard Conditions of Sale-Immediate Purchasers Outside the United States"), 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 the seller's entire 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 (or Price Sheet 153), 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 (OR PRICE SHEET 153) 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 (or PRICE SHEET 153).

Understanding Several types of safety-alert messages may appear throughout this instruction sheet and on labels and tags attached to the TripSaver II Communications Gateway. Become familiar with these Safety-Alert types of messages and the importance of these various signal words: Messages A 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. A WARNING "WARNING" identifies hazards or unsafe practices that can result in serious personal injury or death if instructions, including recommended precautions, are not followed. **A** 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. If any portion of this instruction sheet is unclear and assistance is needed, contact the nearest Following S&C Sales Office or S&C Authorized Distributor. Their telephone numbers are listed on S&C's Safety website sandc.com, or call the S&C Global Support and Monitoring Center at 1-888-762-1100. Instructions NOTICE Read this instruction sheet thoroughly and carefully before installing the TripSaver II Communications via Gateway system. Replacement If additional copies of this instruction sheet are required, contact the nearest S&C Sales Office, S&C Authorized Distributor, S&C Headquarters, or S&C Electric Canada Ltd. Instructions and Labels It is important that any missing, damaged, or faded labels on the equipment be replaced immediately. Replacement labels are available by contacting the nearest S&C Sales Office, S&C Authorized Distributor, S&C Headquarters, or S&C Electric Canada Ltd.

Location of Safety Labels



Reorder Information for Safety Labels

Location	Safety Alert Message	Description	Part Number
Α		This control is connected to electrical distribution equipment	180-000070-00 Rev A
В		Risk of electric shock	180-002533-01
С		Earth Ground	180-002577-01
D		Enclosure must be grounded	180-000710-01



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
	• (Optional) An ac power cable
Inspection	Examine the shipment for external evidence of damage as soon after receipt as possible, preferably before removal from the carrier's conveyance. Check the bill of lading to make sure the listed shipping containers are present.
	If there is visible loss and/or damage:
	1. Notify the delivering carrier immediately.
	2. Ask for a carrier inspection.
	3. Note the condition of shipment on all copies of the delivery receipt.
	4. File a claim with the carrier.
	If concealed damage is discovered:
	1. Notify the delivering carrier within 15 days of receipt of shipment.
	2. Ask for a carrier inspection.
	3. File a claim with the carrier.
	Also, notify S&C Electric Company in all instances of loss and/or damage.
Handling	
	DO NOT drop the communications gateway or subject any of its parts to undue stress during installation. Only remove the communications gateway from the carton when you are ready for installation. The communications gateway weighs about 25 lbs. (11.4 kg); follow proper lifting techniques to avoid minor injury.
Storage	TripSaver II Communications Gateways are shipped on pallets banded with plastic wrap. This packaging is designed to protect the communications gateway from freight damage. This packaging is not suitable for outdoor storage because it can pool water and damage the communications gateway. After receipt, TripSaver II Communications Gateways should be stored indoors in their shipping packaging. Storing communications gateways outdoors in the shipping packaging will void the warranty.
Returning	If for any reason the communications gateway is to be returned, place it in the original shipping carton to prevent damage during shipping. If additional shipping cartons are required, contact the nearest S&C Sales Office, S&C Authorized Distributor, or S&C Headquarters.



Figure 1. The TripSaver II Communications Gateway.

Mounting the Communications Gateway to a Pole

Follow these steps to mount the communications gateway:

- **STEP 1.** Attach the communications gateway in an upright position, with the S&C logo facing you, to the pole using the upper and lower mounting bolts provided. See Figure 1 on page 8 and Figure 2.
- **STEP 2.** Connect a #2 copper (or equivalent) ground wire from the base of the communications gateway to the ground rod.



Figure 2. Mounting the communications gateway to the utility pole.

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

Powering the Communications Gateway

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.



Figure 3. The communications gateway control PS/Battery Board.

- **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 9.
- **STEP 5.** After a short delay, LEDs on the PS/Battery board and the gateway controller should light up, indicating the communications gateway is receiving power. See Figure 1 on page 8 and Figure 3.

Note: A user-supplied disconnect switch may be required for your installation between the ac input and the PS/Battery board. Contact the nearest S&C Sales Office for details. See the power system diagram (Figure 72 on page 77).

Securing the Communications Gateway To secure the communications gateway, close the door and use the door latches to secure the enclosure. See Figure 2 on page 9. The door latches accept locks with a maximum shackle diameter of %-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.

	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 Kit 903-002702-02/01" section on page 15 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 [%] ₂ -inch nuts.
	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 th	nese 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 11.
	STEP 2.	Remove the existing field-area network radio. See Figure 4 on page 11.
		(a) Disconnect the power plug from its receptacle.
		(b) As applicable, disconnect the Ethernet connector or the serial connector from the receptacles on the radio.
		(c) Disconnect the antenna connector.
		(d) Remove the radio from the mounting plate.
	STEP 3.	Install the new radio. Follow the procedure outlined in the "Installing a New Radio" section on page 11.
		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 14.

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.
 - (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.
- Prince Connector Springloaded screw Connector LED light on PS/ Battery board
- (c) Install the top bracket using the four nuts.

Figure 5. Disconnect the ac line fuse and install the battery.

- **STEP 3.** Connect the battery. With the ac line fuse still removed, connect the red and black battery leads to the white 2-pin connector on the PS/Battery board. The acrylic safety cover over the PS/Battery board does not need to be removed to make this connection.
- **STEP 4.** 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 confirms the battery is functioning.
- **STEP 6.** Reconnect the ac-cable connector.

Replacing a Battery

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

- **STEP 1.** Disconnect the ac power cable connected to the bottom of the gateway (See Figure 2 on page 9) and then disconnect the ac line fuse located at the lower right corner of the gateway box. See Figure 5 on page 13.
- **STEP 2.** Remove the 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 PS/Battery board. See Figure 5 on page 13.
 - (b) Unscrew the four 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 "Installing a New Battery" section on page 13.



Figure 6. Battery installation.

Installing Remote Antenna Kit 903-002702-02/01

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

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.



Figure 7. Do not block antenna drain holes.

- **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.



Figure 8. The remote antenna.

Installing Remote Antenna Kit 903-002701-01/02 The 890- to 960-MHz, 10-dBi antenna includes an omnidirectional Yagi antenna, a pole-mounted single antenna arm with 30-foot (9.1-m) or 50-foot (15.2-m) coaxial cable, and N-type male connectors on both ends. The customer must provide 1.375-inch (35-mm) OD pipe for the antenna.

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

- **STEP 1.** Install the antenna on the antenna bracket.
- **STEP 2.** Attach the antenna bracket to the pole to the specified azimuth, per the network design. The pole should not block the line of sight to other antennas.
- **STEP 3.** Slip the supplied cold-shrink tube over the antenna cable and connect the end where the shrink tube was applied to the antenna. Tighten finger-tight.
- **STEP 4.** Wrap the cable connector inside the antenna with one piece of vinyl mastic tape. Don't stretch excessively, and do not block the antenna drain holes.
- **STEP 5.** Apply the second piece of tape overlapping the end of the first piece and tightly cover the cable end of the connector.
- **STEP 6.** Align the end of the cold-shrink tube flush with the bottom of the antenna and shrink it over the tape and cable.
- **STEP 7.** Tie-wrap the cable to the antenna bracket. 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	The 403- t male con	to 470-MHz, 2-dBi antenna includes an omnidirectional antenna with an N-type nector.
904-002450-02	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	STEP 1.	Visually inspect the antenna for damage (bent, not vertical).
Antenna	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.	$Follow \ the \ procedure \ outlined \ in \ the \ previous \ ``Installing \ Local \ Antenna'' \ section.$

Software User's Guide Logging on to the Communications Gateway

The communications gateway is accessed via a Web browser interface. Connect a personal computer (PC) with a CAT5 Ethernet cable to the communications gateway's Ethernet Port 1. See Figure 4 on page 11. 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.

Command Prompt	_	×
DNS Servers		^
10.20.16.232		
NetBloS over Tcpip Enabled		
Ethernet adapter Ethernet 3:		
Connection-specific DNS Suffix . :		
Description Realtek USB GbE Family Controller #2		
Physical Address 54-BF-64-1A-D1-E2		
DHCP Enabled Yes		
Autoconfiguration Enabled : Yes		
IPv4 Address		
Subnet Mask		
Lease Obtained		
Lease Expires		
Default Gateway		
DHCP Server : 192 168 1 1		
NetBios over Tcpip Enabled		

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

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

NOTICE

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

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

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



Figure 11. The Communications Gateway Login screen.

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

NOTICE

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

TripSaver® II Communication Dateway	Profile			
Logost	Current User Profile You are using in order to acc	the default password. Y	You must change the password to a non-default value change it now to proceed.	
	User:	admin		
	Current Password:	2000000000	0	
	New Password:	20020000000	0	
	Confirm New Password:	2000000000	0	
		Apply		

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

After a successful login, the browser will open to the communications gateway General Status screen with an application Navigation menu on the left side of the screen. The Navigation menu will remain visible for all subordinate menu interface screens. See Figure 15 on page 24.

Enabling IEC 60870-5-104 Communication Protocol in the Communications Gateway The communications gateway is shipped configured to use the DNP3 communication protocol by default. Before starting to configure the communications gateway, S&C recommends first switching to the IEC 60870-5-104, or "IEC104," protocol. To switch to the IEC104 protocol:

- **STEP 1.** Select "Gateway Settings" from the **Navigation** menu.
- **STEP 2.** Scroll down to the SCADA Protocol panel. Click on the **IEC104** radio button. See Figure 13.

STEP 3. Scroll up to the top of the screen and click the **Save** button.

TripSaver* II Commonities Common	Gateway Settings				
General Status Gateway Settings Device Management	General Gateway Settings				+
TripSaverill II Service Center Configuration Software Remote Drop Open	Gareney Name stand_acce				
GangLocal Operation ENP3 Master Settings ENP3 Outstation Settings	Ethernet I (LAN)		Ethornet 2 (WAN)		
User Roles Security Settings Profile	Static IP Address 192:168:1.1 NetMask	Ping Krepana	DBICP Claust	Ping Response	
Degenetics	255 255 555 0 DBCP Server Co. O DBCP Server Start IP Address				
	192-168.1.10 DBICP Server End IP Address 1922-168.1.20				
	SCADA Protocol		Time Synchronization		
	Сомр • КСом		Time Synchronization Searce Time Sync from Unit Device	GPS only	

Figure 13. The IEC104 Protocol panel and Save button.

A success message will display, and the **IEC104 Setpoints**, **IEC104 Controlling Station**, and **IEC104 Controlled Station** menu items will show on the menu bar. See Figure 14.

TripSaver® II Communication Gateway	Gateway Settings
	DICT SETTER LINUT ADDRESS
General Status	192.168.1.20
Gateway Settings	
Device Management	
TripSaver@ II Service Center	
Configuration Software	SCADA Protocol
Remote Drop Open	O DNP3
Canal acal Operation	IEC104
Gang/Local Operation	
User Roles	
IEC104 Setpoints	
IEC104 Controlling Station	
IEC104 Controlled Station	Cold Restart / Reset Process
Security Settings	
Profile	
Diagnostics	

Figure 14. IEC104 enabled.

General Status

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, S&C strongly recommends only one of those users be assigned the admin role. S&C also strongly recommends 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.

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

The *General Status* screen is comprised of the "Gateway Identity," "GPS," "Gateway LAN," "Gateway WAN," "Gateway Hardware," and "SCADA Communication" panels. The "Gateway Identity" panel contains five fields: **Gateway Name**, **Gateway Serial #**, **Gateway Software Version**, **Gateway App Version**, and **Gateway Platform Version**. The "GPS" panel contains five fields: **Status**, **Time Since Last GPS Fix**, **Location**, **Satellites (In Use)**, and **System Time**. The "Gateway LAN" and "Gateway WAN" panels contain three fields each: **Link Status**, **IP Address**, and **Netmask**. The "Gateway Hardware" panel contains four fields: **Battery Present**, **Battery Health**, **Battery Voltage (Volts)**, and **Door Status**. The "SCADA Communication" panel contains the **IEC 104 Communication Status** field. See Figure 15.

Gateway Identity		GPS	
Gateway Name	lec104demo	Status	Available
Gateway Serial Number	M1001403	Time Since Last GPS Fix	00.00:00
Gateway Software Version	4.1.00335	Location	41° 59' 59.10113" N 87° 40' 38.1567" W
Gateway App Version	2023.10.02 15:06 CDT 6416/6182	Satellites (in Use)	6 (4)
Gateway Platform Version	7.1.2-1.2.7.1	System Time	Wed, 11 Oct 2023 15:21:29 GMT
Gateway LAN		Gateway WAN	
on Link Status	lin	Link Status	Un
IP Address	192 168 1 1	IP Address	10.24.140.125
Netmask	255 255 255 0	Netmask	255.255.254.0
Gateway Hardware			
Battery Present	Yes		
Battery Health	Operational		
Battery Voltage (Volts)	13.59		
Door Status	Open		

Figure 15. The General Status screen.

Gateway Settings

The *Gateway Settings* screen contains the "General Gateway Settings," "Ethernet 1 (LAN)," "Ethernet 2 (WAN)," "SCADA Protocol," "Time Synchronization," "Gateway Configuration," "Firmware Upgrade," "Reboot Gateway," and "Ping Station" panels.

Note: For all field edits within each menu, the Save button must be clicked on for field modifications to occur. See Figure 16.

TripSaver* II	Gateway Settings			
General Status Galeewy Settings Device Management Trip Saverti II Service Center Configuration Software Remote Drop Open	General Gateway Settings Gateway Nume Demo Gateway			
Gang/Local Operation User Roles IEC104 Setpoints	Ethernet 1 (LAN)		Ethernet 2 (WAN)	
IEC164 Controlling Station IEC164 Controlled Busion Security Settings Frontin Chapmattes	Static IP Address 102 108 1.1 NetStatic 200 205 205 0 DICP Server DICP Server DICP Server (State IIP Address) 102 108 1.10 DICP Server Valle IP Address 102 108 1.20	Pag Royanor	NBCCP Cliner Stattic IP Address 102:168:20:100 Defusito Gareeray IP Address 102:168:20:1 Neeklask 200:255:255:0	Pag Reparts
=	SCADA Protocol		Time Synchronization Time Synchronization Source	GPS only v
	Gateway Configuration	Expert Configurations	Tane Spar From User Device	
	Firmware Upgrade			
	Uphaal Farmare File	Upper		
	Reboot Gateway			
	© Reboot			
	Ping Station 700 102 106 52 100			
	© 3&C Electric Company 2021			148-4-0-00270

Figure 16. The Gateway Settings screen.

General Gateway Settings

The "General Gateway Settings" panel contains the **Gateway Name** field that allows unique naming of the communications gateway.

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 17.

TripSaver® II Communication Externey	Gateway Settings	
General Status		Save
Gateway Settings		
Device Management	General Gateway Settings	
TripSaverill II Service Center Configuration Software	Gateway Name	
Remote Drop Open	Lemo Generally	
Course and Courses		

Figure 17. The Gateway Name field in the "General Gateway Settings" panel.

Ethernet 1 (LAN)

In the "Ethernet 1 (LAN)" 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 18. 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 **Static IP Address**, **NetMask**, and **DHCP Server** fields require identification.

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

TripSaver* II Contrastation Contender	Gateway Settings				
General Status	Ethernet 1 (LAN)		Ethernet 2 (WAN)		÷
Gateway Settings	Static IP Address	Ping Response	DBCP Client	Ping Response	
Device Management	192.168.1.1	CIM 💽	(C)	State of the second sec	
Thp Saverti II Service Center Configuration Software	NetMask		Static IP Address		
Remote Drop Open	255,255,255,0		152 168 20 100		
Gang/Local Operation	DBCP Server		Default Gateway IP Address 192, 168 20, 1		
User Roles	DHCP Server Start IP Address		NetMask		
IEC104 Setpoints	192.168.1.10		255 255 255 0		
IEC104 Controlling Station					
IEC104 Controlled Station	DITCP Server Lad IP Address				
Security Settings	194, 199, 1, 20				

Figure 18. The "Ethernet 1 (LAN)" panel.

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 the 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.

Ethernet 2 (WAN)

The "Ethernet 2 (WAN)" 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 19.

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.

TripSaver* II Control or attention	Gateway Settings				
General Status	Ethernet 1 (LAN)		Ethernet 2 (WAN)		
Gateway Settings	Static IP Address	Ping Response	DBCP Client	Ping Response	
Device Management	192.168.1.1	- CN 🕥	(a) core	() err	
TripSaverili II Service Center	NetMask		Static IP Address		
Exercise David Group	255 255 255 0		192 168 20 100		
Canal ceal Costation	DBCP Server		Default Gateway IP Address		
United Robert	CN		192, 168, 20, 1		
Uper Holes	DHCP Server Start IP Address		NetMask		
EC104 Costrolling Station	192.168.1.10		255 255 255 0		
IEC104 Controlled Station	DHCP Server End IP Address				
Enclosed and the state of the s	192.168.1.20				
secondy semings					
Profile					
Diagnostics					

Figure 19. The Ethernet 2 (WAN) fields.

DHCP State 'Off'

Three fields require identification: **Static IP Address**, **Default Gateway IP Address**, and **NetMask**. The **Static IP Address** field is the WAN IP address assigned to the communications gateway. The **Default Gateway IP Address** field is the address of the network device "up-stream" of the communications gateway via Ethernet Port 2. All IEC104 traffic sent to the IEC104 controlling station will be routed through this default gateway.

DHCP State 'On'

No fields require identification. The communications gateway will initiate a DHCP request to the WAN's DHCP server, which will assign an IP address for all data communications over the WAN. See Figure 20.

TripSaver® II Control or Stationary	Gateway Settings				
General Status	Ethernet 1 (LAN)		Ethernet 2 (WAN)		
Gateway Settings	Static IP Address	Ping Response	DBCP Client	Ping Rasponse	
Device Management	192 168 1 1	CIN 💽	CN 🔘		
TripSaveril II Service Center Configuration Software	NetMask				- 1
Remote Drop Open	255 255 255 0				
Gang/Local Operation	DBCP Server				
User Roles	DHCP Server Start IP Address				
IEC104 Setpoints	192 358 1 30				
IEC104 Controlling Station					
IEC104 Controlled Station	DBCP Server End IP Address				
Security Settings	192.168.1.20				
Profile					
Diagnostics					

Figure 20. 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. Scroll up and click on the **Save** button to make changes.

SCADA Protocol

The communications gateway supports the use of the IEC 60870-5-104 protocol, or "IEC104" protocol, which is a separate communications protocol to the **DNP3** protocol the communications gateway uses by default. To switch to the **IEC104** protocol, select the **IEC104** radio button and then click on the **Save** button. To switch back to DNP3, select the **DNP3** radio button and then click on the **Save** button. Instructions can also be found in the "Enabling IEC 60870-5-104 Communication Protocol in the Communications Gateway" section on page 23. See Figure 21.

TripSaver" II	Gateway Settings					
rel Status vay Bettings	192.166.1.20					
e Managemeer wer® II Service Center paration Software	SCADA Protecol			Time Synchronization		
	Covrs 9 scron			Time Synchronization Source Trace Spice From Core Device	GPS only	
Selpointa Controlling Station Controlled Station	Cold Restart / Rest Process			IEC104 Time Zone		
r Settings Hica				(-soci utc		
	Gateway Configuration	1	Experi Configuration			
	Firmware Upgrade					
	Ciplant Pressure Pile	$\{T_{1,n}^{i} \mapsto k\}$	(Transfer			

Figure 21. The SCADA protocol selection.

Note: Instructions for configuring the communications gateway using the DNP3 protocol (including the **DNP3 Cold Restart/Reset** feature) are located in S&C Instruction Sheet 461-509, "TripSaver® II Cutout-Mounted Recloser; Communications via Gateway using the DNP3 Protocol: *Installation, Operation, and Configuration.*"

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

Time Synchronization

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

The communications gateway also supports a fourth method of time synchronization. To perform a one-time synchronization from the user's computer accessing this Web interface, click on the **Time Sync From User Device** button. This will immediately sync the gateway's clock to the time in the user's computer. After this one-time synchronization, the gateway will continue to use its configured **Time Synchronization Source** setting to maintain its clock in the future. This option could be useful for lab purposes or for initial system deployment. See Figure 22.

TripSaver* II Democratic Cateroy	Gateway Settings		
General Status			
Gateway Settings	SCADA Protocol	Time Synchronization	
Device Management	ODNP	Time Synchronization Source	GPS only
TripSaventi II Service Center Configuration Software		Time Sync From User Device	GPS only BCADA only
Remote Drop Open			GPS primary, SCADA backup M
GangiLocal Operation			

Figure 22. The "Time Synchronization" panel.

IEC 104 Time Zone

The drop\down **IEC 104 Timezone** field that allows a user to select the local time zone so it can be synchronized with whatever the SCADA time is set for **Single/Double** commands and spontaneous transmission events.

Time Synchronization Source and IEC 104 Time Zone Configuration Options Table 1 identifies the recommended **Time Synchronization Source** and **IEC 104 Time Zone** settings when the SCADA master is providing timestamps using local time.

	•	• •	
No.	Time Synchronization Source	IEC 104 Time Zone	Comments
1	GPS only	Local Time Zone	Recommended
2	SCADA only	(+0.00) UTC	Recommended
3	GPS Primary, SCADA Backup	Any	Not recommended
4	SCADA only	Any	Not recommended

Table 1. Time Synchronization Settings Options

When using option 3 or 4, the TripSaver II Communications Gateway could experience a high number of reboots because of a large time-synchronization delta. As such, these configuration options are not recommended.

When the SCADA master is providing timestamps using UTC time, the **IEC104 Time Zone** field must be configured as "(+0.00) UTC" to prevent rejection of **Single/Double** commands.

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 **Expor**t 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. Selecting either the **Import Configuration** or **Export Configuration** option invokes a series of dialog boxes allowing PC navigation to a configuration file for "Import" or the saving of a file for "Export." See Figure 23.

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

TripSaver® II	Gateway Settings				
General Status	SCADA Protocol		Time Synchronization		
Gateway Settings	O DNP		Time Synchronization Source	GPS only	
Device Management			Time Sync From User Device		
TripSaver® II Service Center Configuration Software					
Remote Drop Open					
Gang/Local Operation	Gateway Configuration				
User Roles					
IEC104 Setpoints	Configuration	Configuration			
IEC104 Controlling Station					

Figure 23. The Import Configuration and Export Configuration buttons.

XML File Description

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

<ConfigDB>

<configuration>

<item value="True" name="gangOperationEnabled"/>

</configuration>

</ConfigDB>

where name="gangOperationEnabled" represents the communications gateway's **Gang Operation** feature, and the associated value="True" indicates the feature is to be enabled. The list of parameters that can be included in the <ConfigDB> section of the XML is detailed in Table 2.

Table 2. Import and Export ConfigDB Parameters

Name	Description	Data Type of Value	Range of Value
IECtoggle	This setting enables the IEC 60870-5-104 protocol for SCADA communication. When set to "True," the gateway communicates via IEC 60870-5-104. When set to "False," the gateway communicates via the alternate DNP3 protocol (not defined in this specification).	Boolean	True or False
timeSyncSource	This setting defines the preferred time synchronization source(s) for the gateway. "gps" indicates the device will only rely on GPS for time synchronization. "scada" indicates the device will only rely on the IEC 104 interface for time synchronization. "gpsScada" indicates the device will use GPS as its highest priority time source but use IEC 104 as a backup if GPS is not available.	String	gps, scada, or gpsScada
devicename	User-specified device name. See the Gateway Name field in Figure 17 on page 26.	String	n/a
gangOperationEnabled	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.	Boolean	True or False
gangOperationMaxRetries	The maximum number of times the gateway will retry a Gang operation after timing out in its initial attempt. Used with gangOperationRetryTime. A value of zero (0) disables the Gang operation retry mechanism.	Integer	0 – 2592000
gangOperationRetryTime	The time interval between Gang operation retry attempts in seconds.	Integer	1 – 3600
enableSingleUnitOperation	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 singe-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.	Binary	True or False
RemoteDropOpenEnabled	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.	Binary	True or False

The second section in the XML file format is encapsulated by $\langle IEC104 \rangle$ tags. This contains all the IEC104 related settings, for example:

<IEC104>

<SinglePoints>

<singlepoint eventsEnabled="1" periodicReportingEnabled="1" interrogationGroup="6" ioa="10000" codeDescription="9"/><singlepoint eventsEnabled="0" periodicReportingEnabled="1" interrogationGroup="0" ioa="10001" codeDescription="4"/>

</SinglePoints>

</IEC104>

The configuration settings that can be specified in this section of the document are described in Table 3.

Parameter Group	Attribute	Description	Data Type	Range of Value
<controllingstations> <controllingstation></controllingstation> </controllingstations>	ipAddress	IP address of the IEC 104 controlling station. One or two IP addresses can be configured. One address is required to establish IEC 104 communication. The gateway will only allow communication with a configured address.	IP address (dotted decimal)	Any valid IP address
<controlledstation> <controlledstation></controlledstation> </controlledstation>	maxAllowableCommandDelay	Maximum allowable time difference, in seconds, between the timestamp received in an IEC 104 command with time and the present gateway system time when the command is received.	Integer	1 to 60
	measuredValuePollingInterval	Time interval between periodic refreshes of measured value setpoints.	Integer	15 to 300
	periodicReportingInterval	Time interval between periodic reports for any setpoints configured for periodic reporting.	Integer	15 to 3600
	backgroundReportingInterval	Time interval between background reports for any setpoints configured for background reporting.	Integer	60 to 14400
	commonAddress	ASDU common address of gateway.	Integer	1 to 65534
	w	Maximum number of IEC 104 APDUs in the receive direction before the gateway will send an acknowledgement.		1 to 32767
	k	Maximum number of IEC 104 APDUs in the transmit direction before the gateway will wait for an acknowledgement.	Integer	1 to 32767
	t1	Timeout for unconfirmed APDUs in the transmit direction.	Integer	1 to 255
	t2	Timeout to send acknowledgment in receive direction.	Integer	1 to 255
	t3	Timeout for sending test frames on an idle connection.	Integer	1 to 172800
	ioa	Information Object Address for this setpoint. Integer value starting at 10000.	Integer	10000 to 19999
	codeDescription	Integer value referring to the setpoint code description defined in S&C Instruction Sheet 461-561.	Integer	Valid values defined in 461-561.
<singlepoints></singlepoints>	eventsEnabled	Indicates whether the gateway will report spontaneous events for this setpoint when the value changes. A value of "1" enables events. A value of "0" disables events.	Integer	0 or 1
<singlepoint></singlepoint> 	backgroundReportingEnabled	Indicates whether the gateway will include this setpoint in its periodic reports. A value of "1" enables periodic reporting. A value of "0" disables periodic reporting.	Integer	0 or 1
	interrogationGroup	Defines the interrogation group that will include this setpoint. When this is set to a value of "0," this setpoint will only be reported as part of overall station interrogation. When this is set to a value of between "1" and "16," this setpoint will be reported as part of overall station interrogation and as part of the specified interrogation group.	Integer	0 to 16

Table 3. Import and Export Settings Configuration

TABLE CONTINUED ►

Table 3. Import and Export Settings Configuration - Continued

Parameter Group	Attribute	Description	Data Type	Range of Value
	ioa	Information Object Address for this setpoint. Integer value starting at 20000.	Integer	20000 to 29999
<doublepoints> <doublepoint></doublepoint> </doublepoints>	codeDescription	Integer value referring to the setpoint code description defined in S&C Instruction Sheet 461-561.	Integer	Valid values defined in 461-561.
	eventsEnabled	Indicates whether the gateway will report spontaneous events for this setpoint when the value changes. A value of "1" enables events. A value of "0" disables events.	Integer	0 or 1
	backgroundReportingEnabled	Indicates whether the gateway will include this setpoint in its periodic reports. A value of "1" enables periodic reporting. A value of "0" disables periodic reporting.	Integer	0 or 1
	interrogationGroup	Defines the interrogation group that will include this setpoint. When this is set to a value of "0," this setpoint will only be reported as part of overall station interrogation. When this is set to a value of between "1" and "16," this setpoint will be reported as part of overall station interrogation and as part of the specified interrogation group.	Integer	0 to 16
	ioa	Information Object Address for this setpoint. Integer value starting at 30000.	Integer	30000 to 39999
	codeDescription	Integer value referring to the setpoint code description defined in S&C Instruction Sheet 461-561.	Integer	Valid values defined in 461-561.
	scaling	Floating point scaling factor. Will be applied as a multiplication factor to the raw setpoint measurement before it is sent to the controlling station.	Float	0.001 to 1000
<measuredvalues></measuredvalues>	fixedDeadband	Fixed deadband interval used to determine when to send a spontaneous event for the measured value setpoint. When the scaled setpoint value changes by the fixed deadband amount, the gateway sends a spontaneous event. A value of 0 (zero) disables fixed deadband checking.	Integer	0 to 50000
<measuredvalue></measuredvalue> 	percentDeadband	Percent deadband interval used to determine when to send a spontaneous event for the measured value setpoint. When the scaled setpoint value changes by the percent deadband amount, the gateway sends a spontaneous event. A value of 0 (zero) disables percent deadband checking.	Integer	0 to 99
	periodicReportingEnabled	Indicates whether the gateway will include this setpoint in its periodic reports. A value of "1" enables periodic reporting. A value of "0" disables periodic reporting.	Integer	0 or 1
	interrogationGroup	Defines the interrogation group that will include this setpoint. When this is set to a value of "0," this setpoint will only be reported as part of overall station interrogation. When this is set to a value of between "1" and "16," this setpoint will be reported as part of overall station interrogation and as part of the specified interrogation group.	Integer	0 to 16

TABLE CONTINUED ►

Parameter Group	Attribute	Description	Data Type	Range of Value	
<singlecommands> <singlecommand></singlecommand> </singlecommands>	ioa	Information Object Address for this setpoint. Integer value starting at 40000.	Integer	40000 to 49999	
	codeDescription	Integer value referring to the setpoint code description defined in S&C Instruction Sheet 461-561.	Integer	Valid values defined in 461-561.	
	retryBehavior	Indicates whether the gateway must retry the command when unsuccessful. A value of "0" enables retries. A value of "1" disables retries.	Integer	0 or 1	
	maxRetryAttempts	The maximum number of times the command will be retried.	Integer	1 to 2,592,000	
	retryInterval	Time in seconds between retry attempts.	Integer	1 to 3600	
<doublecommands> <doublecommand></doublecommand> </doublecommands>	ioa	Information Object Address for this setpoint. Integer value starting at 50000.	Integer	50000 to 59999	
	codeDescription	Integer value referring to the setpoint code description defined in S&C Instruction Sheet 461-561.	Integer	Valid values defined in 461-561.	
	retryBehavior	Indicates whether the gateway must retry the command when unsuccessful. A value of "0" enables retries. A value of "1" disables retries.	Integer	0 or 1	
	maxRetryAttempts	The maximum number of times the command will be retried.	Integer	1 to 2,592,000	
	retryInterval	Time in seconds between retry attempts.	Integer	1 to 3600	

Table 3. Import and Export Settings Configuration - Continued

Import Configuration

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

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

TripSaver® II Comparison Gallery	Gateway Settings	Import Configuration		×
General Status	Gateway Configuration	Choose File No file chosen		
Gateway Settings	Import Configuration			_
ThipSaverili II Service Center Configuration Software	Firmware Upgrade			Ingent
Remote Drop Open Gang/Local Operation	Upload Firmware File	Tippale	Land	
User Roles				
IEC104 Controlling Station				

Figure 24. The Import Configuration dialog box.

52 TripSaver* II	Gat	Gateway Settings			-						
Continuoration Galleen		saaring seminge				Import Configuration			×		
General Status	C Open										×
	e - · · •	> This	c					~ ð	P Search This PC		
Gateway settings	Organice +								E.	- 11	0
Device Management	This PC	1.	Folde	rs (7)							-
TripSaver® II Service Cent Configuration Software	30 Objects Desitop			30 0	bjects		Desktop				l
Remote Drop Open	Documents	i.	2	Deci	ments		Downloads				
Gang/Local Operation	Pictures	Ų		h Mus		0	Pictures				
		Filenam	•						XML Document (*.)	umi)	-
IEC104 Controlling Station									Open	Cancel	3

Figure 25. Import file navigation.
Export Configuration

Follow these steps to complete the **Export Configuration** function. See Figures 26 and 27.

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

TripSaver® II Communication Coloney	Gateway Settings	Export Configuration		×
General Status Gateway Settings Device Management	Gateway Configuration	File name textFile		
TripSaver® II Service Center Configuration Software	Firmware Upgrade			Eaport
Gang/Local Operation User Roles	Upload Financare File	Spender	Carro	
IEC104 Serpoints				

Figure 26. The Export Configuration dialog box.

TripSaver® II Continuenties Converge	Gateway Settings			
General Status				
Gateway Settings				
Device Management	Gateway Configuration			
TripSaverti II Service Center Configuration Software	Insport Configuration	Esport Configuration		
Remote Drop Open				
User Roles	Firmware Upgrade			
IEC104 Selpoints	Upload Famouan File	Court		
🗋 testfile.ani 🧄				Show all X

Figure 27. Export File Save navigation.

Firmware Upgrade

The "Firmware Upgrade" panel enables the loading of firmware versions onto the communications gateway. See Figure 28. 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 28.

Figure 28. The Firmware Upgrade panel.

STEP 3. A Windows dialog box will open. See Figure 29. Navigate to the firmware file and select it. Click on the **Open** button.

© Open X						
← → • ↑	> This	PC > Desktop > Communications Gateway Firmware		ٽ ~		ications Gat
Organize 🔻 Ne	ew folder				<u>}</u> == ▼	
- Ouisk assess	^	Name	Status	Date modified	Туре	Size
Dropbox	*	FCG-4.0.00225.a2b6fdb.2021-03-17-11.16-ota.signed.img	0	3/25/2021 4:22 PM	Disc Image File	106,632 KB
Desktop	*					
🕹 Downloads	*					
🔮 Documents	*					
o Creative Clou	u 🖈					
E Pictures	* 🗸 -	¢				>
	File na	me: FCG-4.0.00225.a2b6fdb.2021-03-17-11.16-ota.signed.img		~	All Files (*.*)	~
					Open	Cancel

Figure 29. The Open File dialog box.

STEP 4. The file loads to the communications gateway. After the upload completes, the gateway will confirm a successful upload. See Figures 30 and 31.

TripSaver® II	Gateway Settings
General Status	Colores Conference
Gateway Settings	Garessay Centigaration
Device Management	Import Expert
TripSaventi II Service Center Configuration Software	Comparison
Remote Drop Open	
Gang/Local Operation	Ermman Lygrade
User Roles	Lipited Farewark Tale Lippede Cannot
IEC104 Setpoints	
IEC104 Controlling Station	33pkuadaki 1.24 MiD / 109.19 MiD (1.09 N)
IEC104 Controlled Station	
Security Settings	
Profile	Reboot Gateway
Diagnostics	
Logent	C Hettoor

Figure 30. The Firmware Upload progress bar.

TripSaver® II Communication Sameway	Gateway Settings
General Status	
Gateway Settings	Gateway Configuration
Device Management	Expert Expert
TripSaver® II Service Center Configuration Software	Coefiguration Coefiguration
Remote Drop Open	
Gang/Local Operation	Firmware Upgrade
User Roles	Optical Termine Fale
IEC104 Setpoints	
IEC104 Controlling Station	Aphaad Completel: Phase Wait.
IEC104 Controlled Station	
Security Settings	
Profile	Reboot Gateway
Diagnostics	
Logout	O Hidoot

Figure 31. The Firmware Upload Complete message.

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 32.

TripSaver® II Connuctation Connector	Gateway Settings
General Status	Comm Conference
Gateway Settings	Gateway Coshguration
Device Management	Import Expert Configuration
TripSaveril II Service Center Configuration Software	Research Res
Remote Drop Open	
Gang/Local Operation	Erminary Opgrade
User Roles	Uplind Temmer File Lippade Carol
IEC104 Setpoints	
IEC104 Controlling Station	Ventication in progress. Photose Wait.
IEC104 Controlled Station	
Security Settings	
Profile	Reboot Gateway
Diagnostics	
Legent	O Heboot

Figure 32. The firmware-verification message bar.

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 33.

TripSaver* II	Gateway Settings
General Status Gateway Settings Device Martagement TripSaventi II Service Center	Gatenay Configuration
Configuration Software Remote Drop Open Gang/Local Operation User Roles IEC164 Setpoints IEC164 Setpoints	Firmware Upgrade System Image VenScation System Image is werked Cick Upgrade button inten mady. CK
IEC104 Controlled Station Security Settings Profile Diagnostics	Reloos Gateway

Figure 33. 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 34 and 35.

TripSaver® II	Gateway Settings
General Status	
Gateway Settings	Gateway Configuration
Device Management	Import Export
TripSaventi II Service Center Configuration Software	- Configuration
Remote Drop Open	Einennen Ummede
Gang/Local Operation	Fillingite C billion
User Roles	Upload Fernance File Upgrade Cancel
IEC104 Setpoints	
IEC104 Controlling Station	Bystem Image Wertkarbün Completed.
IEC104 Controlled Station	
Security Settings	
Profile	Reboot Gateway
Diagnostics	
Legot	C. MELCON

Figure 34. The Upgrade button in the "Firmware Upgrade" panel.

TripSaver® II Connuctation Connector	Gateway Settings
General Status Gateway Settings Device Management ThpSaventi II Service Center	Gateway Configuration Import Configuration Configuration Configuration
Configuration Software Remote Drop Open Gang/Local Operation	Firmware Upgrade
IEC104 Setpoints IEC104 Controlling Station IEC104 Controlled Station	Liggend i annan fra Liggend Cause Liggende in progress. Plane Vont 🔿
Security Settings Profile Diagnostics Legicol	Reboot Gatemay

Figure 35. The firmware-upgrade process progress bar.

STEP 8. When the gateway has completed processing the upgrade, it will display a notification. See Figure 36. 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 log-in page after the reboot completes. Log in and confirm the new firmware has been installed successfully by going to the *General Status* screen.



Figure 36. The dialog box showing the firmware upgrade is complete.

Reboot Gateway

The red **Reboot** button enables the user to restart the communications gateway. See Figure 37. When selected, a dialog box appears to confirm the **Reboot** command. After the user clicks on the **OK** button, the user interface will display the *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.

TripSaver® II Communication Galence	Gateway Settings
General Status	
Gateway Settings	
Device Management	Raboot Gatenay
TripSaver® II Service Center Configuration Software	
Remote Drop Open	
Gang/Local Operation	
User Roles	Pier Station
IEC104 Setpoints	
IEC104 Controlling Station	Pag 902 168.52 100
IEC104 Controlled Station	

Figure 37. The Reboot Gateway button.

Ping Station

The **Ping Station** feature will allow the user to ping the SCADA controlling station or any connected IP address. This feature allows to user to confirm the gateway is correctly connected to the user's network. Type in the IP address of the SCADA controlling station or other device and click on the **Ping** button. See Figures 38 and 39. A "Success" message will appear, and the results of the ping will display as text in the "Ping Station" panel. If the ping is unsuccessful, a "Results" message will appear in the panel showing what went wrong.

TripSaver* II patholistetise tassety	Gateway Settings	
General Status Gateway Settings Device Management Thip Service Center Conference on Service	Rebust Gatenay	
Remote Drop Open GangiLocal Operation User Roles	Ping Station 702 102 102 103 100	
IEC104 Setpoints IEC104 Controlling Station IEC104 Controlled Station Security Settings	© SdC Electric Chaptery 2021	var 4.0.00210

Figure 38. Location of the Ping Station button.



Figure 39. A ping results message.

Device Management

The purpose of the **Device Management** menu is to provide the ability to add (pair), 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 from the communications gateway will remove the recloser's wireless communications capability. To re-enable wireless (**Gateway** mode), the TripSaver II recloser 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 "Service Center Pairing a TripSaver II Recloser with Firmware Version 1.8 or Later" on page 71 for a description of the pairing process.

To add a TripSaver II recloser, click on the **Add TripSaver II** button on the top right of the screen. A dialog box will appear. Enter the recloser's transceiver ID and the desired device name. See Figure 40 and Figure 41 on page 46. 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* screen 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 "Service Center Pairing a TripSaver II Recloser with Firmware Version 1.8 or Later" on page 71.

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

General Status. Seal of a manufacture of a m	TripSaver* II Communication Enterney		Add TripSaver# II Cutou	t-Mounted Recloser	×	
tig banke Chang Rende Drop Open Genigeration Stations Genigeration Stations GEO16 Contracted Stations Security Stations	General Status Gateway Settings Device Management	Secul # TripSever Manage A	Transceiver ID TripSaver II Device Name	conscision accessoon.	Add Tripliner® II Calori M	ounied Rectioner
Usar Kalas MC Nik Agennis MC Nik Agennis MC Nik Controlled Station Security Settings Putter Chapterstes	Trip Sarverili II Service Center Configuration Software Remote Drop Open Gang/Local Operation	Redoer		Card	OC Zoneov Ldz	
KC104 Controlling Station KC104 Controlling Station KC104 Controlling Station Records Settings Provide Diagnostics Teams	User Roles IEC104 Setpoints					
Security Settings Profile Displayments Tenerry	IEC104 Controlling Station					
Dagenetes	Security Settings Profile					
5 14C Earth Country 30) ver(6 00)0	Diagnostics	8 IAC Electric Connects 3037				ver 4.0.00310

Figure 40. Pairing of a TripSaver II recloser with the communications gateway.



Figure 41. The *Device Management* screen showing the successful addition of a TripSaver II recloser and status.

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

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

TripSaver® II ServiceWICenter ConfigurationconSoftwarewipla

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 S&C Instruction Sheet 461-504 for more information about operation of the service center configuration software.

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

NOTICE

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

To enable connection to the service center configuration software, click on the **Enable Service Center Configuration** toggle button to set the **On** position. See Figure 42.

TripSaver* II Contract Star Larrowy	TripSaver® II Service Center Configuration Software	
General Status Gateway Settings Device Management TripEovertil I Barvice Center Configuration Software Remote Dring Open GangLocal Operation User Roles IEC104 Belpuonts	Service Center Configuration Configuration	
IEC104 Controlling Station	0.3&C Zincrei Company 2022	82 -

Figure 42. The Enable Service Center Configuration toggle button.

When the **Service Center Configuration** mode is enabled, a dialog box appears. See Figure 43.

Sc TripSaver* II	TripSaver® II Service Cer		
Centeral Status Catevory Settings Device Management ThypEarcerth II Service Center Configuration Software Nemete Dropo Open Cang Local Operation Locar Roles IEC106 Setpoorts	Service Center Centiguration Easthe Service Center Configuration Easthe Service Center Configuration	Enable SCC access via Etherner port 1 The devoe may take a lew momenta to apply the change.	
IEC104 Controlling Station	© 54 C Electric Company 2021		sur 4 8 00218

Figure 43. The "Enable SCC access via Ethernet port 1" dialog box.

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 44 on page 48.

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 serve 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.

File Connection	Data	Tools	Help						
2 2 2 2		×	14	Q	۹.		🗸 Validate	Apply	Kevert Revert
S&C TripSa Cutout-Mo Reclos	ver® II unted er								
TCC Curve Settin	igs								
NR Curve Setting									
Sectionalizing Se									
LCD Screen Setti									
Communication	Connect t	o Device							
Local Manual Op			TripSav	ver II		Device Name	Status		
			TCMR-97	406		Marengo Ave TripSaver II Recloser	Available		
						Identify	Connect Cancel	Ī	
×		Transce	iver ID:						

Figure 44. The service center configuration software Connect to Device screen.

Remote Drop Open

TripSaver II reclosers supplied with the **30-second** option ("-O") and firmware version 1.8 or later, and ordered with the **Remote Drop Open** option ("-D") factory-enabled, can be configured using the **Remote Drop Open** settings to operate when issued an **IEC104** 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 "IEC104 Controlling Station" section on page 62 for directions on configuring the gateway with an IEC104 controlling station.

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 IEC104 points must also be set. For a full list of the IEC104 points available, refer to S&C Instruction Sheet 461-561, "TripSaver® II Communications Gateway, Outdoor Distribution (15 kV and 25 kV): *IEC 60870 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," and "TripSaver II recloser #3." Document this information along with the device names for later use when setting IEC104 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 45 on page 49.

TripSaver® II Commune alter Gateway	Remote Drop Open							
General Status								
Gateway Settings								1000
Device Management	Remote Drop Open Settin	igs						Sere
TripSaver® II Service Center Configuration Software	Total Design Design of Career							
Remote Drop Open	Enable Remote Drop Open in Galeway	ON O	-					
Gang/Local Operation				Activa	te RDO			
User Roles	Barto Marco		Factory	Activated in	Activated in	RDO	Receive Gang	Gang RDO
IEC104 Setpoints	Device Name	Serial	T5II	TSII	GW	Status	RDO	Status
IEC104 Controlling Station	Marengo Ave TripSaver II Recloser	TCMR-97406	YEA	CRI 🔵	CN 💽	- 63%	ON 🔵	05
IEC104 Controlled Station								
Security Settings			T				Canal Line C	Disp Oyen Zirtras
Profile								
Diagnostics								
Legest								
	© S&C Electric Company 2023							ver 4.0.00033

Figure 45. Enabling the Remote Drop Open feature in the communications gateway.

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.

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 46.

TripSaver® II Communication Gateway	Remote Drop Open							
General Status								
Gateway Settings								-
Device Management	Remote Drop Open Settin	igs						5410
TripSavent: II Service Center Configuration Software								
Remote Drop Open	Enable Remote Drop Open in Gateway	CRN 💽						
Gang/Local Operation				Activat	te RDO			
User Roles		122	Tactory	Activated in	Activated in	RDO	Receive Gang	Gang RDO
IEC104 Setpoints	Device Name	Serial	TSH	TSII	CM.	Status	RDO	Status
IEC104 Controlling Station	Marengo Ave TripSaver II Recloser	TCMR-97406	YES-	ce 🔵	ON 🔵	.08	ON 🔵	on
IEC104 Controlled Station								
Security Settings				T	- T		Carriel Report 1	hop Open Retries
Protile								
Diagnostics								
Legest								
	© 5&C Electric Company 2021							ver.4.0.00033

Figure 46. Activating the Remote Drop Open feature in the TripSaver II recloser and the communications gateway.

To allow the recloser to gang-operate because of a **Gang Remote** command, toggle the **Receive Gang RDO** toggle button to the **On** position. Click on the **Save** button to save the settings. Up to three reclosers can be configured to remotely gang-operate in response to an IEC104 **Communications Gateway Remote Gang Drop Open** command. See Figure 47.

seral Status								
leway Settings								
vice Management	Remote Drop Open Settin	ngs						-1410
Saventi II Service Center								
note Drog Open	Enable Remote Drop Open in Gateway	CH 🔵						
va/Local Operation				100	0.00			
r Roles			Tactory	Activat	# RDO	RDO		Gang RDO
104 Setpoints	Device Name	Serial	Enabled in TSH	TSII	GW GW	Activation Status	RDO RDO	Activation Status
04 Controlling Station	Marengo Ave TripSaver II Recioser	TCMR-97406	YER	ON O	ON O	ON	ON O	ON
04 Controlled Station			-					100 million (100 million)
rity Settings							Carrot Reserve 2	top Open Returns
ile								
nostics								

Figure 47. Enabling a 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 48.

TripSaver® II Construction Category	Remote Drop Open							
General Status								
ateway Settings								
evice Management	Remote Drop Open Setti	ngs						5417
ripSaver® II Service Center								
onnyurauon sonware	Enable Remote Drop Open in Gateway	OH C						
and and Grantian								
				Activa	00X st	100		6 m 1990
ser Koles	Device Name	Serial	Explicit in	Activated in TSII	Activated in GW	Artivation	Receive Gang EDO	Activation
C104 Setpoints	Building 142 Trintman & Bardinan	1/1/2474/4	174	C201	1.300		C100	
C104 Controlling Station				1. dente	ALC: NO		N. CONTRACTOR	
C104 Controlled Station								
curity Settings							Carrier Connect	hop open fortune
otile								
agnostics								
legent								
	© S&C Electric Company 2021							ver.4.0.000

Figure 48. A TripSaver II recloser when the Remote Drop Open feature is not factoryenabled in the recloser.

Gang/Local Operation

Local Drop Open Settings

TripSaver II reclosers supplied with firmware versions 1.7 and later can be configured using the **Local Drop Open** settings to drop open when another member of the configuration group, or "gang," drops open because of a permanent fault, a **Local Manual Open** (**LMO**) operation, or an orientation change. (These operations are overseen directly by the gateway and are not signaled by a SCADA controlling station via IEC104.) This feature is called **Gang Operation**. If no backup battery is available in the communications gateway enclosure, this screen will be disabled. See Figure 49.



Figure 49. The communications gateway requires a backup battery for Local/Gang operation.

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

When toggled on, the **Enable Single Unit Operation** button 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 on 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 50 on page 52.



Figure 50. Enabling the single-unit Local Drop Open operation.

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

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

The **Enable in Gateway** toggle button must be set to allow the gateway to gang-operate the TripSaver II recloser, while the **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 an IEC104 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 51 on page 53.

eneral Status			Sec
dearay Cattions			
vice Management	Local Drop Open Operation Se	ttings	
pSaver® II Service Center onfiguration Software	Enable Single Unit Operation		
mote Drop Open	Enable Gang Operation	on •	
ang/Local Operation			
er Roles	Local Drop Open Retry Time	to Each ganglocal drop open operation retry	
C104 Setpoints	(seconds)	will occur at an interval of 00:00:10 (hours intrudes : seconds)	
C104 Controlling Station			
C104 Controlled Station	Local Drop Open Max Retries	Retry Time and Max Retries settings result. 3500 in a maximum overall retry time of	
curity Settings	(monther)	00:10:00:00 (days : hours : minutes : seconds)	
ofile			
agnostics			
Logost		Initiate Gang Operation Open	
	Name	Serial Permanent LMO Orientation Enable in Enable in Include in Perform Local	
	Marengo Ave TripSaver II	Fault Change Gateway II Gang Command	
	Recloser	TCMR-97406	

Figure 51. Enabling a Gang operation.

Two other features that should be configured are the **Local Drop Open Retry Time** and the **Local Drop Open Max Retries**. See Figure 52.

TripSaver® II Communication Converse	Gang/Local Opera	tion	
General Status Gateway Settings Device Management	Local Drop Open Operation Set	tings -	Text
TripSaver® II Service Center Configuration Software	Enable Single Unit Operation	la or	
Remote Drop Open	Enable Gang Operation		
User Roles IEC104 Setpoints	Local Drop Open Retry Time (secondi)	10 Each gang/local drop open operation retry will occur at an interval of 00.00510 (hours minutes: second)	
IEC104 Controlling Station IEC104 Controlled Station	Local Drop Open Max Retries (attempts)	Retry Time and Max Retries settings result 5600 in a maximum overall retry time of	
Security Settings Profile		00:1000:00 (days : hours : minutes : seconds)	
Diagnostics			
Legost	Name	Initiate Gang Operation Receive Local Drop Open Sertial Permanent LMO Orientation Enable in Include in Perform Local Fault Change Gateway II Gang Command	
	Marengo Ave TripSaver II Recloser		
	Per	Gaust Day Open Keyes	

Figure 52. Configuring the Retry Time and Maximum Number of Retries settings.

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

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.

A WARNING

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

The **Cancel Drop Open Retries** button will be enabled when a **Gang Operation** procedure is active and performing periodic retries. When this button is clicked, the communications gateway will immediately halt the retries and will abandon the **Drop Open** operation. See Figure 53.



Figure 53. Performing a Gang Trip operation.

A TripSaver II recloser and a paired communications gateway can be configured for both **Single Unit Operation** and **Gang Operation** functions. See Figure 54.

TripSaver" II Communication Communic	Gang/Local Opera	tion			
General Status Gateway Settings Device Management	Local Drop Open Operation Set	tings			lave
TripSaver® II Service Center Configuration Software	Enable Single Unit Operation	он 🌍			
Remote Drop Open Gang/Local Operation	Enable Gang Operation				
User Roles IEC104 Setpoints	Local Drop Open Retry Time (seconds)	10	Each gangflocal drop open operation retry will occur at an interval of 00:00:10 (hours minutes (seconds)		
IEC104 Controlling Station IEC104 Controlled Station Security Settings Profile	Local Drop Open Max Retries (attempts)	3600	Retry Time and Max Retnes settings result in a maximum overall retry time of 00:10:00:00 (carys : hours : minutes : seconds)		
Diagnostics					
Leger	Name Marengo Ave TroSaver II Reciber Tro	Serial TCMR-974 Rem Gang Trip	Initiate Gang Operation Permanent Fault LMO Change Informed Composition Composition	Receive Local Drop Opin Canade in Busto In Cataviary The Server Canag Command The Cataviary Common Cataviary Common Cataviary Common Cataviary Common Cataviary Common Cataviary	

Figure 54. A Single Unit and Gang operation.

User Roles

The purpose of the **User Roles** menu is for adding users and corresponding access privileges. The types of user roles include Admin, Gateway User, TripSaver II User, and Technician. The addition of a user is initiated by clicking on the **Add User** button. A dialog box will appear with the required **User**, **Password**, and **Confirm Password** fields, and a drop-down box to select user type. See Figure 55 and Table 4 on page 56.

TripSaver® II	User Roles	Add User			×		
General Status		User.	user name				
Gateway Settings		Password	000000000	0		Addition	
Device Management		Contine Descuret		0			
TripSaver® II Service Center Configuration Software		a commence		U		Action	
Remote Drop Open		Role	Admin	*			
Gang/Local Operation			Galeway User TripSaver II User	Ð	Canod Add		
User Roles			Technician				
IEC104 Setpoints							
IEC104 Controlling Station							
IEC104 Controlled Station							
Security Settings							
Profile							
Diagnostics							
Legent							
	© 5&C Electric Company 2021						ver-4,0.00210

Figure 55. The User Role configuration screen.

Page	Element Within Screen	Admin Role	Gateway User Role	TripSaver II User Role	Technician Role
General Status	All	Allowed	Allowed	Allowed	Allowed
Gateway Settings	Update gateway configuration	Allowed	Allowed	Allowed	Allowed
	Install firmware	Allowed	Blocked	Blocked	Blocked
Device Management	Add/Update/Remove TripSaver II recloser buttons	Allowed	Allowed	Allowed	Blocked
Remote Drop Open	All	Allowed	Blocked	Blocked	Blocked
Gang/Local	Configure Gang Operation settings	Allowed	Allowed	Blocked	Blocked
Operation	Perform Gang Trip/ Cancel Gang Trip buttons	Allowed	Blocked	Blocked	Blocked
TripSaver II Service Center Configuration Software	All	Allowed	Blocked	Allowed	Blocked
User Roles	All	Allowed	Blocked	Blocked	Blocked
IEC104 Setpoints	All	Allowed	Allowed	Blocked	Blocked
IEC104 Controlling Station	All	Allowed	Allowed	Blocked	Blocked
IEC104 Controlled Station	All	Allowed	Allowed	Blocked	Blocked
	Configure secure tunnel	Allowed	Allowed	Blocked	Blocked
Security Settings	Provision HTTPS server certificate	Allowed	Allowed	Blocked	Blocked
	Enable remote Web UI access	Allowed	Blocked	Blocked	Blocked
Profile	All	Allowed	Allowed	Allowed	Allowed
Diagnostics	All	Allowed	Allowed	Allowed	Allowed

Table 4. User Role Permissions

IEC 104 Setpoints

Single Point Information Setpoint Configuration

The *Single Point Information Setpoint Configuration* screen contains configuration parameters for single-point information setpoints. The window can be opened by clicking on the **Single Point Information** button. See Figure 56.

TripSaver* Il Connectation Laborat	IEC104 Setpo	ints						
eral Status way Settings ce Management	IEC104 Setpoints							
aventi II Service Center garation Software	Single Point Loo	emarina 🗇 Double Point Informa	m 🛛 Measured Value, doort disating 🕲 Single Command			Double Command		_
e Drop Ogen	Single Point Inform	aution						
Local Operation								
toles.	104	Cada Decorphon		Interruption Group	Background Reporting Coattact		Event Enabled	
l Selpoints	10000	8: Communication Gateway remote w enabled	eb user interface access	0	No		Yes	- Î
Controlling Station	10001	E Communication Gateway remote w enabled via SCA	eb user interface access DA	p.	tio		Yes	
	10002	Select,	Dewir.			- 🖬 🖬	Yes	
Sector (Sector)	10003	Select	Select. 1 Conmunication Galeway runn	ing on primary AC power		-	Yes	
	10004	Select	 Communication Gateway now Communication Gateway is or Communication Gateway don 	ring on Saltery Sackup power Noe I is plant			Yes	
bes	10005	Select	5 Communication Gateway Talls 6 Communication Gateway Talls	ny is present na ballery require replacement			Yes	
<u>1</u>	10006	Select	 Communication Gateway ents Communication Gateway ents Communication Gateway ents 	eleneo CPS synchronization de veis user interface access enabled de veis user interface access enabled via 10	2404		Yes	
	10007	Select	10 Conmunication Gateway we 11 Continuation Gateway we	t user interface to being accessed 5 user interface authentication rejected			Yes	
	10008	Select	12 Control and allon Galeway con 12 Control unication Galeway con 14 Control unication Galeway con	réguration changed via web user interface inguration tile imported intervation tile imported			1975	
	10009	Select.	15 Continuing above Galerway set 16 Continuing above Galerway set	cure furner added			Yes	
	10010	Select	17. Communication Gateway sec 18. Communication Gateway frm	cue tunnel eletoved Invale uppade success			Yes	

Figure 56. Single Point Information setpoint configuration.

The single-point setpoint variables are described as follows:

IOA: IEC 104 Information Object Address. These values are assigned automatically as setpoints and are mapped on this page.

Note: Single-point and double-point variables can be enabled as required, but the same code description cannot be configured on both the single-point page and the double-point page. Configuring the same point on both pages is blocked.

Code Description: These 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 461-561. Code descriptions are defined by selecting the **Code Description** field in line with the respective **IOA** field. A drop-down dialog box will appear with code definitions for all TripSaver II reclosers paired with the communications gateway. See Figure 56. 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.

Interrogation Group: This group defines the interrogation group that will include this setpoint. When set to a value of "0," this setpoint will only be reported as part of overall station interrogation. When set to a value of between "1" and "16," this setpoint will be reported as part of overall station interrogation and as part of the specified interrogation group.

Background Reporting Enabled: This indicates whether the gateway will include this setpoint in its background reports. A **Yes** value enables background reporting. A **No** value disables background reporting.

Events Enabled: This indicates whether the gateway will report spontaneous events for this setpoint when the value changes. A **Yes** value enables events. A **No** value disables events.

Double Point Information Setpoint Configuration

The *Double Point Information Setpoint Configuration* screen contains configuration parameters for double point information setpoints. The screen can be opened by clicking on the **Double Point Information** button. See Figure 57.



Figure 57. Double-point information setpoint configuration.

The double-point setpoint variables are described as follows:

IOA: IEC 104 Information Object Address. These values are assigned automatically as setpoints and are mapped on this page.

Note: Single-point and double-point variables can be enabled as required, but the same code description cannot be configured on both the single-point page and the double-point page. Configuring the same point on both pages is blocked.

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 461-561. Code descriptions are defined by selecting the **Code Description** field in line with the respective **IOA** field. A drop-down dialog box will appear with code definitions for all TripSaver II reclosers paired with the communications gateway. See Figure 57. 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.

Interrogation Group: This group defines the interrogation group that will include this setpoint. When set to a value of "0," this setpoint will only be reported as part of overall station interrogation. When set to a value of between "1" and "16," this setpoint will be reported as part of overall station interrogation and as part of the specified interrogation group.

Background Reporting Enabled: This indicates whether the gateway will include this setpoint in its background reports. A **Yes** value enables background reporting. A **No** value disables background reporting.

Events Enabled: This indicates whether the gateway will report spontaneous events for this setpoint when the value changes. A **Yes** value enables events. A **No** value disables events.

Measured Value, Short Floating Setpoint Configuration

The *Measured Value*, *Short Floating Setpoint Configuration* screen contains configuration parameters for **Measured Value**, **Short Floating Value** setpoints. The screen can be opened by clicking on the **Measured Value**, **Short Floating** button. See Figure 58.



Figure 58. Measured Value, Short Floating setpoint configuration.

The **Measured Value**, **Short Floating** setpoint variables are described as follows: **IOA:** IEC 104 Information Object Address. These values are assigned automatically as

setpoints and are mapped on this page. Code Description: Point codes representing specific measured value points may be

Code Description: Point codes representing specific measured value points may be assigned to individual SCADA point numbers. A full list of code-description definitions is found in S&C Instruction Sheet 461-561. Code descriptions are defined by selecting the **Code Description** field in line with the respective **IOA** field. A drop-down dialog box will appear with code definitions for all TripSaver II reclosers paired with the communications gateway. See Figure 58. 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.

Scaling: A floating point-scaling factor is used to match the measured value input requirements of the SCADA system. This will be applied as a multiplication factor to the raw setpoint measurement before it is sent to the controlling station. If the **Fixed Deadband** option is enabled for a measured value setpoint, the scaling factor will be applied before the **Fixed Deadband** limits are checked.

Pct Deadband: This field creates a range based on a percentage of the last reported value for this measured value point. The range boundary is defined by multiplying the **Percent Deadband** value against the last reported value of the measured value point. In the case where the next measured value exceeds the range either by a positive or

negative amount, the gateway will generate a spontaneous event. The default value is "0" (zero), which disables the deadband comparison. No range is created and no comparison occurs. Specifying a nonzero value creates the range and enables deadband comparison.

Fixed Deadband: This field creates a fixed deadband range relative to the last reported value for this measured value point. In the case where the next measured value exceeds the range either by a positive or negative amount, the gateway will generate a spontaneous event. The default value is "0" (zero), which disables the deadband comparison. No range is created and no comparison occurs. Specifying a nonzero value creates the range and enables deadband comparison.

Interrogation Group: This group defines the interrogation group that will include this setpoint. When this is set to a value of "0," this setpoint will only be reported as part of overall station interrogation. When this is set to a value of between "1" and "16," this setpoint will be reported as part of overall station interrogation and as part of the specified interrogation group.

Periodic Reporting Enabled: This indicates whether the gateway will include this setpoint in its periodic reports. A **Yes** value enables periodic reporting. A **No** value disables periodic reporting.

Single Command Setpoint Configuration

The *Single Command Setpoint Configuration* screen contains configuration parameters for single command setpoints. The screen can be opened by clicking on the **Single Command** button. See Figure 59.

SC TripSaver® II Contraction Coloney	IEC104 Setpoints							
eneral Status aleway Settings evice Management	IEC104 Setpoints							
pSaver® II Service Center Infiguration Software	Single Point Information	Double Point Information	Measured Value, ther	et floating	Single Command		🔁 Double Commu	ba
mote Drop Open	Single Command							
ng/Local Operation								
r Roles	104	Code Des	cription	Retty Denavour	Retty Interval	Ma	Retry attempts	
104 Setpoints	40000	1. Communication Gateway saids	remote web user interface zh	Discard immediately	10		3600	- î
104 Controlling Station	40001	Selec	1. Seeci.				- 🗹 🖾	
104 Controlled Station	40002	Selec	Select. 1: Communication Gate	way remote web user interface aw	ιcπ.		2600	-
urity Settings	40003	Selec	3. Remote NR mode AU 4. Community after Test	L switch command	mand	5	3600	- 1
-	40004	Selec	1001 Remote NR mode 1002 Gateway drop opt	switch for TripSaver II recipper #1 en enable for TripSaver II recipper	41		3600	-
rostics	40005	Selec	1000 Communication p 2001 Remote NR mode	ateway remote single-unit Drog Os switch for TripSaver II recioner #2	en command for Trip[2	laver II reciper #1	3600	-
	40006	Selec	2002 Communication p 2003 Communication p 3001 Remote NR mode	en enable for impS2WFIII RECODER atteway remote single-unit Drop Or siswitch for TricS2wFIII recipter #2	er command for Trip5	laver II recipser #2	3600	-
	40007	Selec	1. 3002 Galeway drop op 3003 Communication p	en enable for TripSaver II recibber ateway remote single-unit Drop Op	#3 en command for Trip!	Laver II recipser #3	3600	- 1

Figure 59. Single Command setpoint configuration.

The Single Command setpoint variables are described as follows:

IOA: IEC 104 Information Object Address. These values are assigned automatically as setpoints are mapped on this page.

Code Description: Point codes representing specific command points may be assigned to individual SCADA point numbers. A full list of code-description definitions is found in S&C Instruction Sheet 461-561. Code descriptions are defined by selecting the **Code Description** field in line with the respective **IOA** field. A drop-down dialog box will appear with code definitions for all TripSaver II reclosers paired with the communications gateway. See Figure 59 on page 60. When a code definition has been chosen, select the **Check Mark** icon to finalize it. Removal of a code selection can be performed by selecting the blank row in the pull-down menu and clicking on the check mark. This will result in the field being displayed as empty. Finally, click on the **Save** button.

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, and the gateway will not retry the command. The **Queue/Retry for a Specified Count** setting will retry the command for the specified **Retry Interval** and **Max Retry Attempts** settings.

Retry Interval: This is the interval, in seconds, between retry attempts. (Range: 1 to 3600)

Max Retry Attempts: This is the maximum number of retry attempts that will be sent. (Range: 1 to 2,592,200)

Double Command Setpoint Configuration

The *Double Command Setpoint Configuration* screen contains configuration parameters for double command setpoints. The screen can be opened by clicking on the **Double Command** button. See Figure 60.

TripSaver" II Communication Category	IEC104 Setpoints						
leneral Status							
ateway Settings	IEC104 Setuciata						
rvice Management	in case in spinis						
lpSaventi II Service Center onfiguration Software	Single Point Information	Double Point Information	Measured Value, short floating	e O Sia	gle Command	Double Cemu	and
emote Drop Open	Double Command						
ang/Local Operation							
ser Roles	104	Code De	scription	Retty Denever	Retty Interval	Max Retry attempts	
000000000000000000000000000000000000000	7303A						
104 Setpoints	50000	Sele	ct. Select.				1
104 Selpoints	50000	Sele	Cl. Select. Select. Cl. 1. Conmunication Gateway rend	fe web user interface switch		✓ ✓ ▲	Í
104 Setpoints	50001	Sele Sele	Cl. Select. Select. 1. Communication Gateway rend 2. Communication Gateway rend 3. Remote NR mode AL select	te web user interface switch te Gang Diop Open comma command	nd	3600 5600	Í
104 Setpoints 104 Controlling Station 104 Controlled Station	50000 50001 50002 50003	Sele Sele Sele	Cl. Select Select Select Con munication Galeway rend Con munication Galeway rend Con munication Galeway rend Con munication Fail TOD: Rendo NN mode watch te TOD: Rendo NN mode watch te TOD: Rendo NN mode watch te	fe with user interface switch to Gang Drop Open comma consumo in TripDaver II recipien #1 for TripDaver II recipien #1	nd Là	> 2600 3600 3600	ĺ
104 Setpoints 104 Controlling Station 104 Controlled Station curity Setlings	50000 50001 50002 50003 50004	Sele Sele Sele Sele Sele	Eleven Seven Seven Seven Seven Seven Seven Communication Galeway rend Communication Galeway rend Communication Galeway rend Communication Real TODI: Rendo NR mode with the TODI: Rendo NR mode with the Communication galeway ct 2015 Rendo NR mode with the Communication galeway	te web user interface switch 6 Gang Drop Open comma command or TrigDaver II recicoser #1 for TrigDaver II recicoser #1 mote single-until Drop Open ir TrigDaver II recicoser #2	nd 12 command for TruSaver II recipeer #	2600 3600 1 2600	1
104 Setpoints 104 Controlling Station 104 Controlled Station curity Settings	50000 50001 50002 50003 50004 50005	Sele Sele Sele Sele Sele Sele	Select. Select. Select. Communication Guideway rend Communication Guideway rend Communication Guideway rend Communication Guideway Communication Guide	fer weiß user infertace switch te dang Drop Open comma contraunce in Trigdaver II recloser #1 for Trigdaver II recloser #2 notb single-unit Drop Open in Trigdaver II recloser #2 for Trigdaver II recloser #2 for Trigdaver II recloser #2	nd Là conn and for TrigSaver II ectober # conn and for TrigSaver II ectober #	C C C C C C C C C C C C C C C C C C C	
2104 Setpoints 2194 Controlling Station 2194 Controlled Station curity Settings attim gnostics	50000 50000 500000 500004 500004 500005	Sele Sele Sele Sele Sele Sele Sele Sele	Benet: 1. 1. Communication Category when a communication Category and communication Category	te web user interface switch te Gang Dop Open comma constante for Tradbaver II nectoar 41 for Tradbaver II nectoar 42 interfaces inge-unit Dop Open interfaces inge-unit Dop Open interfaces inge-unit Dop Open interfaces inge-unit Dop Open interfaces in sectoar 42 for Tradbaver II nectoar 43 for Tradbaver II nectoar 43	nd Là command for TrigSaver II rectoper a command for TrigSaver II rectoper a command for TrigSaver II rectoper a	2 3600 2 3600 2 3600 2 3600 2 3600	
C104 Setpoints C194 Controlling Station C104 Controlled Station curity Settings atile Ignostics	5000 5000 5000 5000 5000 5000 5000 500	See	Servit. Servit. 1. Construction Cultures years 2. Construction Cultures years 3. Construction Cultures years	de web user infortace swich de Gang Dop Open comma constant for TrigGaver II reclaser 41 for TrigGaver II reclaser 42 indos single-unit Dop Open tri TrigGaver II reclaser 42 indos single-unit Dop Open fort TrigGaver II reclaser 43 for TrigGaver II reclaser 43 for TrigGaver II reclaser 43 for TrigGaver II reclaser 43 for TrigGaver II reclaser 43	nd L2 conin and for TrySaver II recoter is conin and for TrySaver II recoter is conin and for TrySaver II recoter is 10	2 2 3000 3600 1 3500 2 3600 3 5600 3 56000 3 5600 3 5600 3 5600 3 5600 3 5600 3 5600 3 5600 3 560	

Figure 60. Double Command setpoint configuration.

The Double Command setpoint variables are described as follows:

IOA: IEC 104 Information Object Address. These values are assigned automatically as setpoints are mapped on this page.

Code Description: Point codes representing specific command points may be assigned to individual SCADA point numbers. A full list of code-description definitions is found in S&C Instruction Sheet 461-561. Code descriptions are defined by selecting the **Code Description** field in line with the respective **IOA** field. A drop-down dialog box will appear with code definitions for all TripSaver II reclosers paired with the communications gateway. See Figure 60 on page 61. 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.

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 and the gateway will not retry the command. The **Queue/Retry for a Specified Count** setting will retry the command for the specified **Retry Interval** and **Max Retry Attempts** settings.

Retry Interval: This is the interval, in seconds, between retry attempts. (Range: 1 to 3600)

Max Retry Attempts: This is the maximum number of retry attempts that will be sent. (Range: 1 to 2,592,200)

IEC104 Controlling Station

The purpose of the *IEC104 Controlling Station* screen is to update the IP settings for connecting to the IEC104 controlling station. The gateway will only allow connections from a configured IP address. To enable communication with the controlling station, IP Address #1 must be set to a valid IPv4 address.

Enter the appropriate IP address in the **IP Address #1 (required):** field. The **IP Address #2 (optional):** field can be configured to support redundancy in the controlling station. See Figure 61.

TripSaver® II Contraction Connection	IEC104 Controlling Stati	on	
General Status	Controlling Station Configuration		200
Device Management TripSaver® II Service Center Configuration Software	IP Address #1 (required): 0.0.0.0	IP Address #2 (optional): 0.000	
Remote Drop Open Gang/Local Operation			
User Noies IEC104 Setpoints IEC104 Controlling Station			
IEC104 Controlled Station Security Settings			
Protile Diagnostics			
Logost	© S&C Electric Company 2021		

Figure 61. IEC104 controlling station configuration.

IEC104 Controlled Station

The IEC104 controlled station defines the configuration settings for the IEC104 protocol. Default values are shown in Figure 62. They are described as follows:

TripSaver* II	IEC104 Controlle	d Station				
General Status Gateway Settings Device Management	Controlled Station Config	uration				
TopSource I Service Conter Configuration Software Remote Drop Open GangU.ccal Operation User Roles RC104 Selponts	ASDU Common Address 1 Background reporting inner 2000	al (Seconde)	Measured value palling interval (Seconds) 15	Cyclic/Periodic reporting interval (Secondo)	Max Aller able Commond Delay (Second) 30	
IEC104 Controlling Station IEC104 Controlling Station Security Settings Prafile Diagnostics	(1 (Seconds) 13	12 (Secondu) 10	d (kenada) 20	k (APBD) 12	* (APDCs) 3	
	6 S&C Electric Company 2021					sue 4.0.00273

Figure 62. IEC104 controlled station configuration.

ASDU Common Address: The application service data unit (ASDU) common address is the address assigned to the gateway for IEC104 communication. (Range: 1 to 65534)

Measured Value Polling Interval (Seconds): This defines the frequency at which the gateway will refresh measured values for reporting to the controlling station. (Range: 15 to 300)

Cyclic/Periodic Reporting interval (Seconds): This is the time between IEC104 cyclic/ periodic reports initiated by the gateway. (Range: 15 to 3600)

Max Allowable Command Delay: This defines the maximum allowed difference between the timestamp provided in an IEC 104 command with time and the present system time. (Range: 1 to 60)

Background Reporting Interval (Seconds): This is the time between IEC104 background reports initiated by the gateway. (Range: 60 to 14400)

t1 (Seconds): This is the timeout for unconfirmed application protocol data units (APDUs), as specified in the IEC 104 standard. (Range: 1 to 255)

t2 (Seconds): This is the send acknowledgement delay, as specified in the IEC 104 standard. (Range: 1 to 255)

t3 (Seconds): This is the keepalive interval, as specified in the IEC 104 standard. (Range: 1 to 172800)

k (APDUs): This is the maximum number of unacknowledged frames in the transmit direction, as specified in the IEC 104 standard. (Range: 1 to 32767)

w (APDUs): This is the maximum number of unacknowledged frames in the receive direction, as specified in the IEC 104 standard. (Range: 1 to 32767)

Security Settings

Secure Tunnel

The communications gateway supports the ability to tunnel all communication network traffic from the communications gateway to a customer-supplied peer. See Figure 63. Enabling a secure tunnel from the communications gateway creates an authenticated, encrypted, and integrity-protected path through which IEC104 traffic will pass.

TripSaver* Il Contractivities famous	IEC104 Controlle	d Station				
General Status Galeway Settings Device Management	Controlled Station Config	uration				
TopSavertil II Service Center Contiguration Software Remote Drop Open Gang4.ocal Operation User Roles IEC104 Selpoints	AMDU Common Address T Background reporting inter- 2000	ral (Seconds)	Manurel value pelling interval (Seenide) 15	Cyclic/Periodic reporting interval (Socondo)	Max Allowable Commond Delay (Seconds)	
IEC104 Controlling Station IEC104 Controlled Station Security Settings Profile Diagnostics	tî (Seconde) 15	12 (Secondi) 10	d Greensky 20	k (APBEs) 12	w (APDC) E	
	© 56C Electric Company 2021					4at 6.0.00273

Figure 63. The Secure Tunnel button.

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

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

OpenVPN Configuration

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

As with the tunnel configuration above, select the **Open VPN** option from the dropdown menu. A configuration dialog box will appear. See Figure 64.

eneral Status						
alarman Settimon	Controlled Station Config	guration				- 7
vice Management						
pSaverII II Service Center Intiguration Software	ASDU Common Address		Measured value polling interval (Seconds)	Cyclic Preiodic reporting interval (Seconds)	Max Allewable Cummand Delay (Secondi)	
mote Drup Open			15	10	10	
eng/Local Operation	Background reporting inter	rval (Seconds)				
er Roles	3600					
C104 Selpcints						
C104 Controlling Station						
2104 Controlled Station	t2 (Secondt)	t2 (Secondri)	(3 (Seconds)	k (APDUs)	w (APDUs)	
curity Settings	15	30	20	12	1	
file						
gnostics						
and the second se						

Figure 64. The Open VPN configuration menu.

Follow these steps to add OpenVPN:

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

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

Remote Web Access

The **Remote Web Access** toggle button enables Web-user interface access via Ethernet Port 2. This configuration setting can only be updated by the admin user and only after the admin user has changed the default password. See Figure 65 on page 66. See the "Enabling Remote Web Access" section on page 66.

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 less. 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 computer: **netsh interface ipv4 set subinterface "Local Area Connection" mtu=500 store=persistent.**

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: from the default password. set to the **On** position. See Figure 65.

- **STEP 1.** In the *Profile* screen, the gateway admin password must be changed locally
- STEP 2. On the Security Settings screen, the Remote Web Access function must be

TripSaver® II Contraction Extension	Security Settings
General Status Galeway Settings Device Management TripsSaverili II Service Center Configuration Software Remote Drop Open GampLocal Operation	Secure Tannel Add Secure Tannel *
User Roles	Remote Web Access
IEC104 Selpoints IEC104 Controlling Station IEC104 Controlled Station Security Settings Protile Diagnostics	
Logost	© 5.6.C Exercise Company 2021 var 6.8.002/0



- **STEP 3.** See Figure 66. On the *IEC104 Setpoints* screen, a **Single Command** or **Double Command** point must be configured with a code description:
 - "1: Communication Gateway remote web user interface switch."

TripSaver® II Communication University	IEC104 Setpoints						
Jeneral Status Saleway Settings Jevice Management	IEC104 Setpoints						
tpSaver® II Service Center onfiguration Software	Single Point Information	Double Point Information	Measured Value, short	floating	Single Command	Doshie Command	
mote Drop Open	Single Command						
ng/Local Operation							
er Roles	104	Code Dep	creilion	Retry Behavior	Retty Interval	Max Retry attempts	
04 Setpoints	4000	1: Communication Gateway swit	remote web user interface th	Discard immediately	10	3600	
104 Controlling Station	40001	Sele	t _a	Discard immediately	10	3600	
104 Controlled Station	40002	Selec	t.,	Discard immediately	10	2600	
unity Settings	40003	Sele	t	Discard immediately	10	3600	
tile	40004	Sele	Su .	Discard immediately	10	3600	
nostics	40005	Sele	<u>K.</u>	Discard immediately	10	3600	
loos	40006	Sele	t.,	Discard immediately	10	3600	
			-				

Figure 66. The remote Web access command point.

- **STEP 4.** See Figure 67. On the *IEC104 Setpoints* screen, two **Single Point Information** or **Double Point Information** 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 enabled via SCADA"

Station Commencement	IEC104 Setpoints							
General Status Gateway Settings Device Management	IEC104 Setpoints					Save		
TripSaver® II Service Center Configuration Software	Single Point Info	ormation 🖸 Double Point Information	🖸 Measure	ed Value, short floating	Single Command	Double Command		
Remote Drop Open	Single Point Inf	ormation						
Gang/Local Operation	KDA.	Code Description		Interrogation Group	Periodic Reporting Enabled	Events Enabled		
IEC104 Setpoints	10000	8: Communication Gateway remote web us access enabled	er interface	0	Yes	Yes		
EC104 Controlling Station	10001	9: Communication Gateway remote web us access enabled via SCADA	er interface	0	Yes	Yes		
ecurity Settings	10002	Select		0	Yes	Yes		
rofile	10003	Setect		9	Yes	Xes		
Diagnostics	10004	Select		<u>0</u>	Yes	Yes		
	10005	Select		0	Yes	Yes		
Logost	10006	Select_		0	Yes	Yes		

Figure 67. The remote Web access status points.

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 less. 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 computer: **netsh interface ipv4 set sub-interface "Local Area Connection" mtu=500 store=persistent.**

- **STEP 6.** From the IEC 104 controlling station, send a single command or double command to the information object address (IOA) configured in Step 3. See Figure 66 on page 67.
- **STEP 7.** At the IEC 104 controlling station, check the **Single Point Information** or **Double Point Information** points configured in Step 4:

"8: Communication Gateway remote web user interface access enabled" point reflects "1"/"True" value.

"9: Communication Gateway remote web user interface access enabled via IEC104" point reflects "1"/"True" value.

STEP 8. When the **Single Point Information** or **Double Point Information** 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. The URL should be the IP address associated with communication gateway's Ethernet Port 2.

Profile

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

TripSaver® II Communication Gammary	Profile	
General Status Galamasy Settings Device Management TopSavell II Service Center Configuration Softwares Remote Drop Open Gangt Coal Operation User Reiss EC104 Setponts IEC104 Controlling Station IEC104 Controlling Station Security Settings	Cense Circ Parla	
Lagost	© 586 Electric Company 2021	5

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.

TripSaver® II Control attent Control by	Diagnostics	
General Status Calency Settings Device Management Typ Same II Service Calenter Configuration Software Remote Drop Open Cangl.ocal Operation User Roles EC104 Controlleng Station EC104 Controlleng Station Security Settings Profile	Diagnostic Logs Resource Tread Log (our Stanue) Retrieve Tread Log (our Stanue) congressed as sign	
Diagnostics	© 56C Ziscin: Computy /021 ver-6.8020	10

Figure 69. The Diagnostics screen.

When any of the **Retrieve** buttons are selected, a dialog box appears with a **Download** and **Cancel** button. See Figure 70. After clicking the **Download** button, a completion bar will display.

TripSaver" II	Diagnostics
Generical Station Gutiencey Settings Device Management Trp:Saver6 II Service Center Centiguration Software Remote Drop Open GampL.coal Operation User Roles IEC104 Setpoints IEC104 Centrolling Station IEC104 Centrolling Station Security Settings Prudite Chapnosities	Response: Log: Response: Log: (con time); Response: Log: (con time); Response: Log: (con time); Dynational diagnosis: Log file: The could take more than a multip to complete. The could take more than a multip to complete.
High	6 SAC Detric Company 2017 verify 2017

Figure 70. The Diagnostic Log download dialog box.

If the **Download** button is clicked, a notification of file download completion appears, and the log file will be saved in the computer's Download file folder. See Figure 71.



Figure 71. The diagnostic log success message.

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

NOTICE

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

A DANGER

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

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

- STEP 3. Connect to the communications gateway with a PC as described in the "Software User's Guide" section on page 19. In the *Device Management* screen, click on the Add TripSaver II button. Fill in the Transceiver ID and TripSaver II Device Name (if desired), and click on the OK button. Note: The device name can be anything but is usually a description of where the TripSaver II recloser is installed.
- STEP 4. When the TripSaver II recloser has been successfully paired, the device will appear in the device listing in the device panel. Periodically refresh the communications gateway's *TripSaver II Device Management* screen using the browser's **Refresh** button. The TripSaver II recloser will be listed as "connected" when pairing is complete. The pairing process could take approximately 5 minutes. If the TripSaver II recloser does not pair, see the "Troubleshooting" section on page 74.
- **STEP 5.** 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 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 or later, 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 or later with a communications gateway already installed in the field.

To perform field-pairing, follow these steps:

STEP 1. Using a PC loaded with Service Center Configuration Software v1.8 or later, 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.

Field-Pairing a TripSaver II Recloser with Firmware Version 1.6 or 1.7 Installed on the Utility Pole and Powered by Line Current
- **STEP 2.** Install the TripSaver II recloser(s) to be paired to the gateway to the utility pole, as described in S&C Instruction Sheet 461-502, "TripSaver® II Cutout-Mounted Recloser, Outdoor Distribution (15 kV and 25 kV): *Installation and Operation*," and power it via line current. Install the communications gateway no more than 30 feet (9.1 m) from the TripSaver II recloser(s) to be paired. Connect the communications gateway to ac power.
- **STEP 3.** Connect to the communications gateway with a PC as described in the "Software User's Guide" section on page 19. In the *Device Management* screen, click on the **Add TripSaver II** button. Fill in the Transceiver ID and TripSaver II Device Name (if desired), and click on the **OK** button. **Note:** The device name can be anything but is usually a description of where the TripSaver II recloser is installed.

When the TripSaver II recloser has been successfully paired, the device will appear in the device listing in the device panel. Periodically refresh the communications gateway's *TripSaver II Device Management* screen using the browser's **Refresh** button. The TripSaver II recloser will be listed as "connected" when pairing is complete. The pairing process could take approximately 15 minutes. If the TripSaver II recloser does not pair, see the "Troubleshooting" section on page 74.

Signal Interference	Difficulties in pairing a TripSaver II recloser with a communications gateway are usually caused by signal interference. Remember, the communications gateway should be no more than 100 feet (30.5 m) away from the TripSaver II recloser and should have an unobstructed view of the recloser. The communications gateway antenna is directional, and the TripSaver II reclosers must be installed above the communications gateway, ideally on the same pole. Also, the heavy use of Bluetooth devices, cellular devices, or Wi-Fi can cause radio interference. If radio traffic is heavy, S&C recommends moving the recloser and communications gateway closer to one another.			
	For optimal performance, install the TripSaver II recloser no more than 30 feet (9.1 m) away from the communications gateway and in direct line of sight.			
Pairing Process Takes Longer Than Expected	Pairing a In some c (after ref resetting following	TripSaver II Cutout-Mounted Recloser should take approximately 5 minutes. cases, it may take up to 15 minutes. If after waiting for 15 minutes the gateway reshing the browser) does not register as "connected," S&C recommends g wireless communications in the TripSaver II recloser by completing the 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: For Overhead Distribution Systems: <i>Protection Setup Using Service Center Configuration Kit.</i> "		
	STEP 3.	Navigate to the Communications Settings menu and select the Communications Mode drop-down menu. Change the Communications mode to the Non-Gateway Mode setting.		
	STEP 4.	Click on the Apply Communications Mode button.		
		Note: The Apply Communications Mode button will not apply any changes that have been made on any other menu screens. If changes have been made to another menu screen, such as the <i>TCC Curve Settings</i> screen, click on the Apply button.		
	STEP 5.	The TripSaver II recloser is now in Non-Gateway mode. Select Gateway mode from the drop-down menu. Click on the Apply Communications Mode button to place the recloser back in Gateway mode.		
	STEP 6.	Connect to the communications gateway, as described in the "Software User's Guide" section on page 19. Remove the TripSaver II recloser's entry on the <i>Device Management</i> screen. Disconnect the TripSaver II recloser from the service center configuration software by clicking on the Disconnect button.		
	STEP 7.	Pair the TripSaver II recloser with the new communications gateway using the instructions in the "Commissioning (Pairing) a TripSaver II Recloser for Use with the Communications Gateway" section on page 71.		

Pre-Installation

- $\hfill\square$ 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
- $\hfill\square$ Make sure the recloser uses firmware v1.6 or later for **Extended Open Interval** functionality.
- $\hfill\square$ Always read the Danger and Warning labels.
- $\hfill\square$ Follow your company's PPE guidelines and standard operating procedures.

Installation

 \Box For the communications gateway, verify:

- 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.

 \Box For the TripSaver II reclosers, verify:

- 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:

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

Interface Pinouts The RS-232 port of the gateway controller module (green box) is configured as data-terminal equipment. See Table 5.

$ \begin{pmatrix} 6 & 7 & 8 & 9 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} $							
Pin	Function	Description					
1	NC	No Connection					
2	RX from Radio	RS-232 Receive					
3	TX to Radio	RS-232 Transmit					
4	NC	No Connection					
5	TX to Radio GND	Signal Ground					
6	NC	No Connection					
7	RTS to Radio Request to Send						
8	CTS to Radio	Clear to Send					
9	NC	No Connection					

Table 5. Gateway Controller Module RS-232 Interface Pinout

Ethernet Ports 1 and 2 use RJ-45 connectors with the pinout shown in Table 6. 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 6. Ethernet Ports Pinout

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

Power System Diagram



Figure 72. The communications gateway power system diagram.

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

Understanding the Radio Mode

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

After pairing the TripSaver II recloser with a gateway using a PC and Ethernet cable, TripSaver II recloser-to-communications gateway functions can be enabled such as **Gang** operation, as well as long-range SCADA functions such as remote SCADA communications, and remote drop open.

Exclusive use of one radio mode at a time is required. The mode is selected by applying the side magnet, cordless power module, and line current in combinations as shown in Table 7 on page 78. Radio activation is different for firmware versions 1.7 or later, so methods for both versions are included in Table 7 on page 78.

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

Cybersecurity–Communications Gateway Radio Mode

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

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

Upon powering up, a TripSaver II recloser will identify itself to the communications gateway and use a secure algorithm to establish an authenticated and encrypted connection to the gateway. The gateway operator must then explicitly add the TripSaver II recloser to the local network via the secure Web-user interface.

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

Gateway Mode Configuration Setting: Enabled or Disabled?	Line Power Available?	Cordless Power Module Available?	Side Magnet Applied?	Side Magnet Configuration Setting: Is Enabled?	Radio Mode (Firmware v1.7)	Radio Mode (Firmware v1.8 and Later)
Disabled	Yes	No	No	•	Radio off	Radio off
Disabled	•	Yes	No	•	USB transceiver	USB transceiver
Disabled	Yes	No	Yes	No	Radio off	Radio off
Disabled	Yes	No	Yes	Yes	USB transceiver	USB transceiver
Disabled	•	Yes	Yes	No	USB transceiver	USB transceiver
Enabled	Yes	No	No	•	Communications gateway	Communications gateway
Enabled	•	Yes	No	•	USB transceiver	USB transceiver
Enabled	Yes	No	Yes	No	Communications gateway	Communications gateway
Enabled	Yes	No	Yes	Yes	Communications gateway	Communications gateway
Enabled	•	Yes	Yes	No	USB transceiver	Communications gateway

Table 7. Radio Mode

① The corded ac power module should never be connected to the TripSaver II recloser when the recloser is powered by line current. See the "Danger" message on page 77. • This could be set to "Yes" or "No" without affecting the **Radio** mode

Gateway Controller Module Indicator Lights



Figure 73. LED indicator lights.

Blue LED: The gateway controller module is connected to power. See Figure 73.

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

Yellow LED: Always On. Reserved for future use.

Regulatory Information

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

United States of America-FCC (Federal Communication Commission)

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

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

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

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

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

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

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

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

Australia/New Zealand (ACMA)

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

Brazil (ANATEL):

Atendimento à Regulamentação Anatel

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

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

Para maiores informações, consulte o site da ANATEL. www.anatel.gov.br

