Wi-Fi Installation

Table of Contents

NOTICE

These instructions are applicable for IntelliRupter fault interrupters shipped after November 15, 2019, with SDA-4554R3-xxx communication modules and firmware versions 2.2 and earlier. For earlier communication modules (R0 communication module), refer to S&C Instruction Sheet 766-522, "S&C IntelliRupter® PulseCloser® Fault Interrupter: For IntelliRupter Installer versions 3.5.0 and later, which can only operate with WiFiAdminInstaller 2.0.0 and later: *Wi-Fi Administration and Operation*."

For firmware versions 3.0 and later, refer to S&C Instruction Sheet 766-528, "IntelliRupter® PulseCloser® Fault Interrupter: Outdoor Distribution (15.5 kV, 27 kV, and 38 kV): R3 Communication Module: *Communication Setup Using Firmware Version 3.0.00512*."

Introduction

Qualified Persons

Read this Instruction Sheet

NOTICE

Thoroughly and carefully read this instruction sheet and all materials included in the product's instruction handbook before installing or operating an IntelliRupter® fault interrupter. Become familiar with the Safety Information and Safety Precautions on pages 4 through 5. The latest version of this publication is available online in PDF format at **sandc.com/en/support/product-literature/**.

Retain this Instruction Sheet

This instruction sheet is a permanent part of the IntelliRupter fault interrupter. Designate a location where users can easily retrieve and refer to this publication.

Proper Application

⚠ WARNING

The equipment in this publication is only intended for a specific application. The application must be within the ratings furnished for the equipment. Ratings for the equipment can be found on the nameplate affixed to IntelliRupter fault interrupter as well as in S&C Specification Bulletin 766-31.

Special Warranty Provisions

shipment, the seller agrees, upon prompt notification thereof and confirmation that the equipment has been stored, installed, operated, and maintained in accordance with recommendations of the seller and standard industry practice, to correct the nonconformity either by repairing any damaged or defective parts of the equipment or (at seller's option) by shipment of necessary replacement parts.

The seller's warranty does not apply to any equipment that has been disassembled, repaired, or altered by anyone other than the seller. This limited warranty is granted only to the immediate purchaser or, if the equipment is purchased by a third party for installation in third-party equipment, the end user of the equipment. The seller's duty to perform under any warranty may be delayed, at the seller's sole option, until the seller has been paid in full for all goods purchased by the immediate purchaser. No such delay shall extend the warranty period.

The seller further warrants to the immediate purchaser or end user that for a period of two years from the date of shipment the software will perform substantially in accordance with the then-current release of specifications if properly used in accordance with the procedures described in seller's instructions. The seller's liability regarding any of the software is expressly limited to exercising its reasonable efforts in supplying or replacing any media found to be physically defective or in correcting defects in the software during the warranty period. Seller does not warrant the use of the software will be uninterrupted or error-free.

For equipment/services packages, the seller warrants, for a period of one year after commissioning, that the IntelliRupter fault interrupters will provide automatic fault isolation and system reconfiguration per agreed-upon service levels. The remedy shall be additional system analysis and reconfiguration of the IntelliTeam® SG Automatic Restoration System until the desired result is achieved.

Warranty Qualifications

The standard warranty contained in seller's standard conditions of sale, as set forth in Price Sheets 150 and 181, does not apply to major components not of S&C manufacture, such as batteries, customer-specified remote terminal units and communication devices, as well as hardware, software, resolution of protocol-related matters, and notification of upgrades or fixes for those devices. The seller will assign to the immediate purchaser or end user all manufacturers' warranties that apply to such major components.

The seller's standard warranty does not apply to any components not of S&C manufacture that are supplied and installed by the purchaser or to the ability of seller's equipment to work with such components.

Warranty of equipment/services packages is contingent upon receipt of adequate information on the user's distribution system, sufficiently detailed to prepare a technical analysis. The seller is not liable if an act of nature or parties beyond S&C's control negatively impact performance of equipment/services packages; for example, new construction that impedes radio communication, or changes to the distribution system that affect protection systems, available fault currents, or system loading characteristics.

Safety Information

Understanding Safety-Alert Messages

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

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

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

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

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

Following Safety Instructions

If any portion of this instruction sheet is unclear and assistance is needed, contact the nearest S&C Sales Office or S&C Authorized Distributor. Their telephone numbers are listed on S&C's website sandc.com, or call the S&C Global Support and Monitoring Center at 1-888-762-1100.

NOTICE	
Read this instruction sheet thoroughly and carefully before configuring the Wi-Fi settings.	

Replacement Instructions and Labels

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.

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.

⚠ DANGER

IntelliRupter PulseCloser Fault Interrupters operate at high voltage. Failure to observe the precautions below 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.

© 1982 NEMA

1. **QUALIFIED PERSONS.** Access to an IntelliRupter fault interrupter 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.

5. **OPERATING MECHANISM AND BASE.** IntelliRupter fault interrupters contain fast-moving parts that can severely injure fingers. Do not remove or disassemble operating mechanisms or remove access panels on the IntelliRupter fault interrupter base unless directed to do so by S&C Electric Company.

6. **ENERGIZED COMPONENTS.** Always consider all parts live until de-energized, tested, and grounded. The integrated power module contains components that can retain a voltage charge for many days after the IntelliRupter fault interrupter has been de-energized and can derive a static charge when in close proximity to a high-voltage source. Voltage levels can be as high as the peak line-to-ground voltage last applied to the unit. Units energized or installed near energized lines should be considered live until tested and grounded.

7. **GROUNDING.** The IntelliRupter fault interrupter base must be connected to a suitable earth ground at the base of the utility pole, or to a suitable building ground for testing, before energizing an IntelliRupter fault interrupter, and at all times when energized.

● The ground wire(s) must be bonded to the system neutral, if present. If the system neutral is not present, proper precautions must be taken to ensure the local earth ground, or building ground, cannot be severed or removed.

8. **VACUUM INTERRUPTER POSITION.** Always confirm the **Open/Close** position of each interrupter by visually observing its indicator.

● Interrupters, terminal pads, and disconnect blades on disconnect-style models may be energized from either side of the IntelliRupter fault interrupter.

● Interrupters, terminal pads, and disconnect blades on disconnect-style models may be energized with the interrupters in any position.

9. **MAINTAINING PROPER CLEARANCE.** Always maintain proper clearance from energized components.

The IntelliRupter fault interrupter Wi-Fi database used by LinkStart v4, LSDBR3.txt is located on the computer at: *C:\Users\Public\Public Documents\S&C Electric\LinkStart*. Each line in the database contains the serial number, device revision, device name, and the device location. This file is automatically created after the first successful LinkStart Wi-Fi connection is made. See Figure 1.
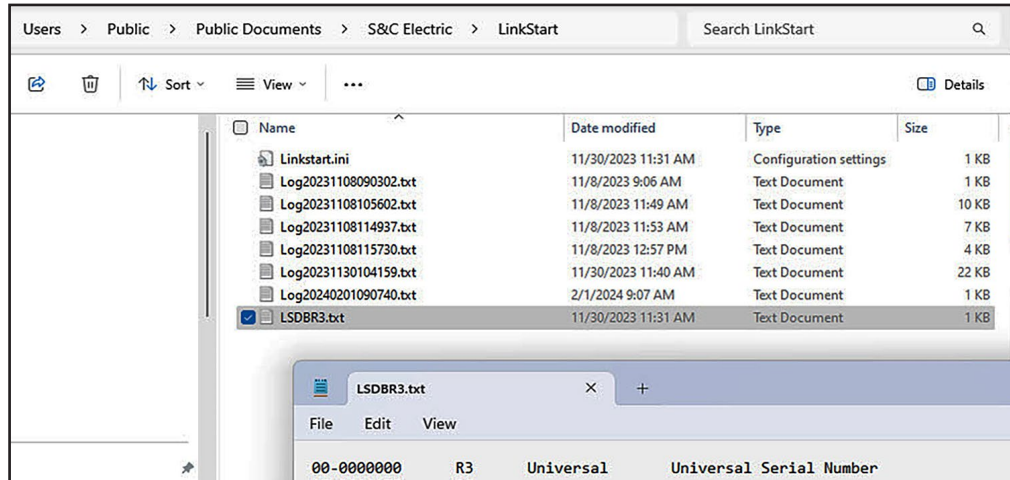

Figure 1. The IntelliRupter fault interrupter Wi-Fi database used by LinkStart v4.

Entries are automatically added to this database file after successful connection to each unique device. To manually add or edit entries using Windows Notepad, double-click on the line to open the file. Each line represents one IntelliRupter fault interrupter. Enter the serial number first (use the format ## – ######), and follow this entry by a tab or one or more spaces. Enter the Wi-Fi communication module version number, either R0 or R3, followed by a tab or one or more spaces. LinkStart v4 will automatically make correction to the version number in this .txt file during the connection process. Enter the name of the IntelliRupter fault interrupter (no spaces are allowed in the device name) and follow this entry by a tab or one or more spaces. Then, enter the device location (spaces may be used).

The universal access number, as illustrated on the first line in Figure 1, should be the first entry in any database. If it is not present, enter this text line: 00-0000000 R3 Universal Serial Number.

NOTICE
The Wi-Fi database structure was changed in LinkStart Version 4.0.0.x. When the existing IntelliRupter fault interrupter database was created for an earlier version of LinkStart, there was no R3 or R0 version number. If the IntelliRupter fault interrupter still has the factory default security keys, the Wi-Fi connection can be completed by entering the IntelliRupter fault interrupter serial number directly into the **Serial Number** field in the LinkStart *Connect to a Device* screen, as shown in Figure 2 on page 7.

Automatic LSDB. txt File Conversion

Copy and paste the old LSDB file to the *ProgramData>S&C Electric>LinkStart* folder. When the LinkStart v4 connects to an R3 Communication Module, a new LSDBR3.txt file will be automatically created in that folder and populated with the existing information from the old LSDB file. A new column is created in the file adjacent to the serial number column to display the "R" revision of the communication module. All serial numbers are initially listed as "R3."

When the LinkStart v4 connects to an IntelliRupter fault interrupter with a serial number that is already in the newly created LSDBR3 file, it always first tries to communicate as though it is an R3 Communication Module. If the IntelliRupter fault interrupter has an R0 module, communication is established and the "R" revision number in the new LSDBR3 .txt file is automatically corrected to display "R0" for that serial number. The universal serial number always remains "R3" because it may connect to any control, first trying R3 and then R0.

Editing the LSDBR3.txt File

Information entered in the LSDBR3.txt file displays in the *LinkStart Connect to a Device* screen when that serial number connects to its IntelliRupter fault interrupter. See serial number 08-9001122 in Figure 2, This text information is displayed in Figure 3.

To demonstrate automatic correction of a manual text entry, when this LSDBR3.txt file was edited the module type was incorrectly entered as "R0." After connecting to that IntelliRupter fault interrupter the LSDBR3.txt file was automatically corrected to "R3," as shown in Figure 4 on page 8.

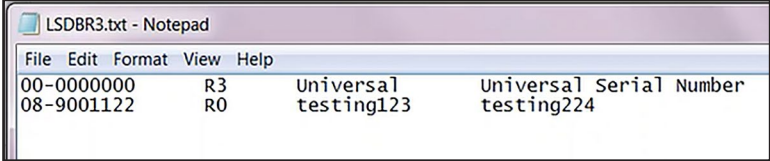**Figure 2. LSDBR3.txt information displayed in the *Connect to a Device* screen.**

Figure 3. The LSDBR3.txt file stored on the computer screen.
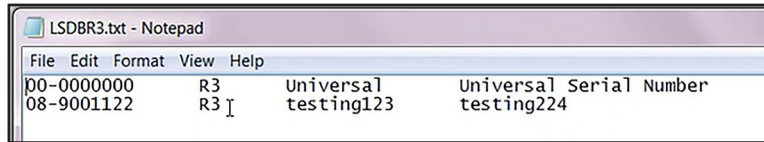
Figure 4. The LSDBR3.txt file is corrected after connecting to serial number 08-9001122.

Converting the Existing LSDB.txt File

When the LinkStart software is connected to an IntelliRupter fault interrupter that has an R3 Communication Module, the existing LSDB.txt file on the computer is automatically converted to the new LSDBR3.txt format and a column is added for the communication module type.

Communication Module Version Change

NOTICE
When LinkStart establishes a connection in the LSDBR3 file, it will attempt to try that connection type for approximately 3 to 5 minutes before trying the alternate connection. This is to allow the most efficient reconnect when a module is removed and reinstalled with LinkStart active. If the communication module type is changed from R3 to R0 or R0 to R3, S&C recommends opening the LSDBR3 database file and editing the connection type to reflect the new module type. This will speed up the connection process. As an alternative, the line containing the IntelliRupter fault interrupter serial number may be deleted. However, changing the connection type will produce a faster connection.

Connecting to the IntelliRupter® Fault Interrupter

Follow these steps to open the *Wi-Fi Configuration* screens in the R3 Communication Module (catalog number SDA-4554R3):

STEP 1. In the Windows® 10 **Start** menu, select *Start>Programs>S&C Electric> Link-Start>LinkStart V4*. The *Wi-Fi Connection Management* screen will open. See Figure 5.
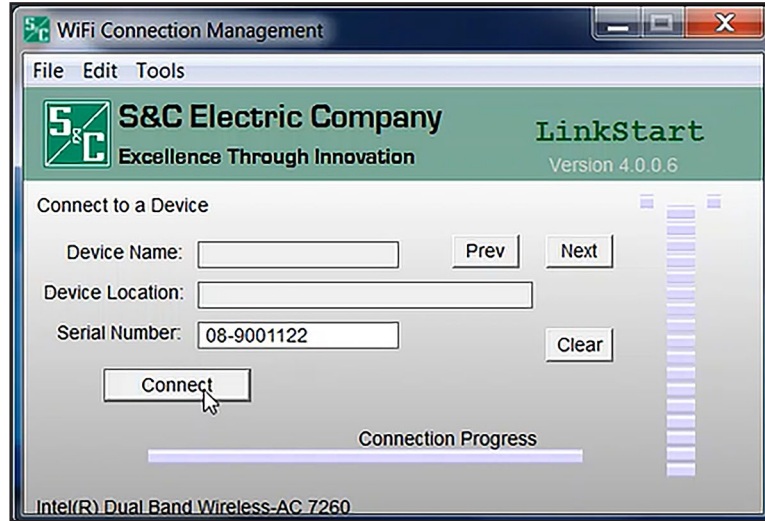

Figure 5. The *Wi-Fi Connection Management* screen.

STEP 2. Enter the serial number of the IntelliRupter fault interrupter and click on the **Connect** button. See Figure 5.

STEP 3. The **Connect** button changes to the **Cancel** button, and connection progress is shown on the Connection Progress status bar. See Figure 6.
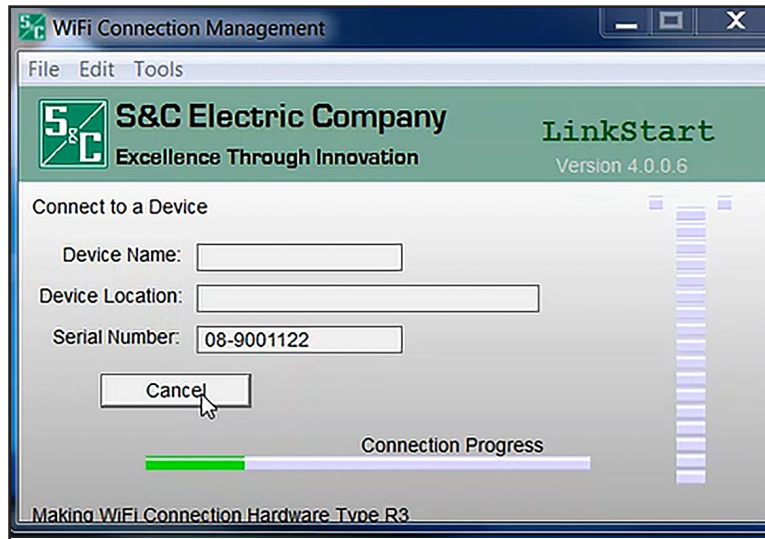

Figure 6. The Connection Progress status bar.

> **STEP 4.** When a connection is established, the status bar indicates "Connection Successful" and displays a solid green bar. The vertical bar graph indicates signal strength of the Wi-Fi connection. See Figure 7.
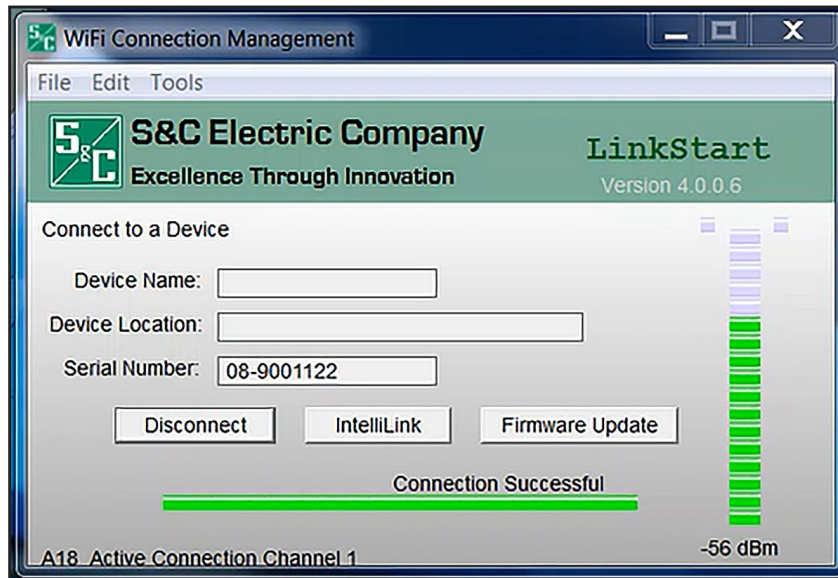

Figure 7. A successful connection to the IntelliRupter fault interrupter.

> **STEP 5.** Open the **Tools** menu and click on the **Wi-Fi Administration** option. See Figure 8.
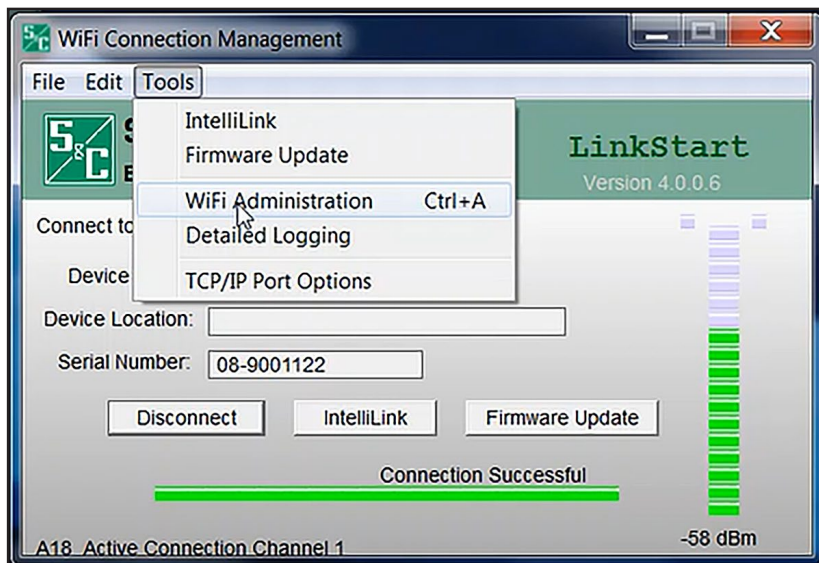

Figure 8. The "Wi-Fi Administration" item on the Tools menu.

Login

The *Login* screen opens requesting a username and password. See Figure 9. These screens are displayed in the Internet browser on the computer. The supported browser versions include Google Chrome and Microsoft Edge. The IP address supplied by the R3 Communication Module is displayed at the top of the screen.

Enter the username and password and click on the **Login** button. Authentication status is displayed.

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/**.
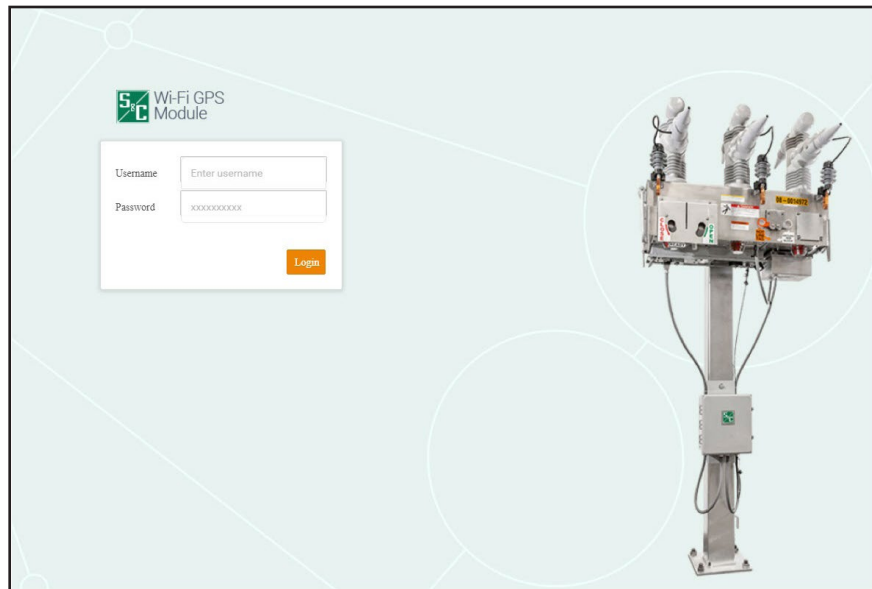

Figure 9. The *Login* screen.

When the default username and password are entered, the *Profile* screen opens and prompts assignment of a new password and confirmation. See Figure 10.
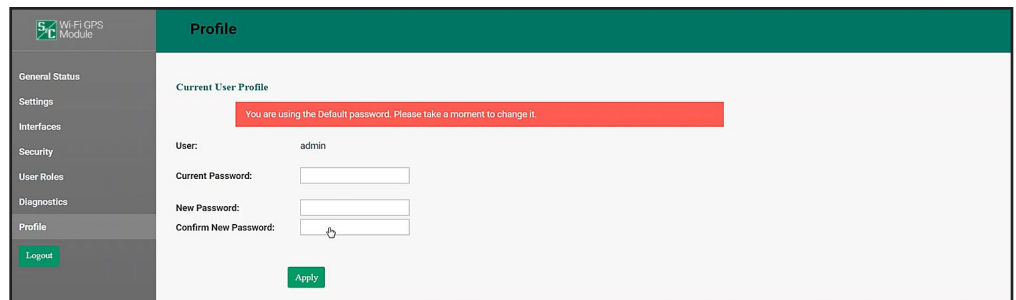

Figure 10. The *Profile* screen.

NOTICE
In firmware versions later than version 2.1, the default user password must be changed before proceeding. This step cannot be skipped because the user cannot navigate to any other page until the password is changed.

With firmware version 2.1 and earlier, to skip this screen and keep the default password setting, click on a menu item in the left menu.
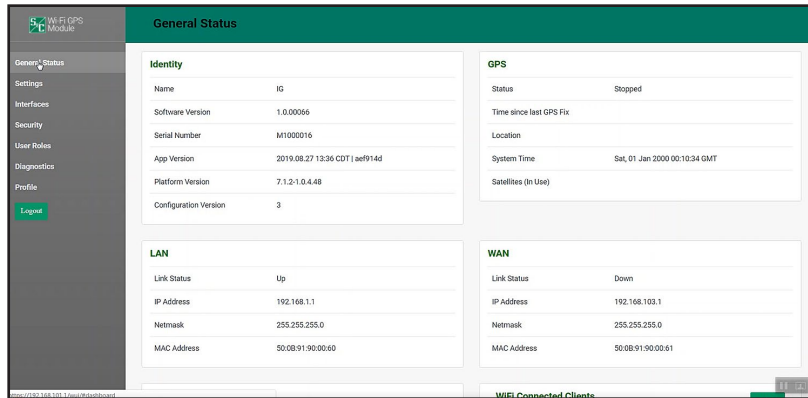

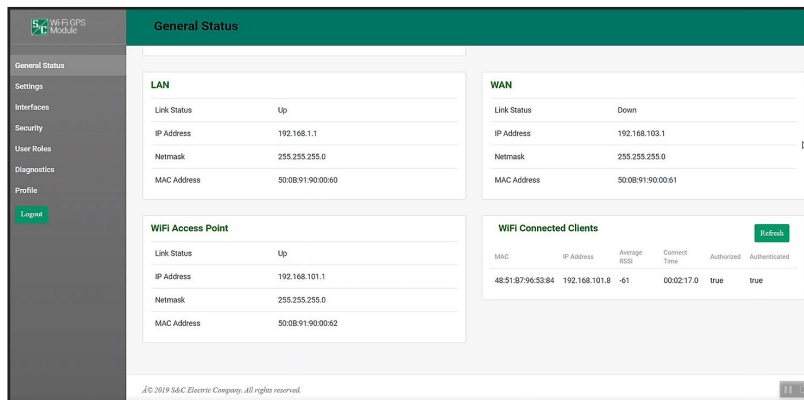**Figure 11. The top of the *General Status* screen.**

Figure 12. The bottom of the *General Status* screen.

General Status

The *General Status* screen is informational and only displays data; no edits are allowed. Field edits are permitted in the respective menu sections where each field is defined. See Figures 11 and 12.

The *General Status* screen is comprised of the Identity, GPS, LAN, WAN, Wi-Fi Access Point, and Wi-Fi Connected Clients panels. The Identity panel contains six fields: **Name**, **Software Version**, **Serial Number**, **App Version**, **Platform Version**, and **Configuration Version**. The GPS panel contains five fields: **Status**, **Time Since last GPS Fix**, **Location**, **System Time**, and **Satellites (In Use)**. The LAN and WAN panels contain four fields each: **Link Status**, **IP Address**, **Netmask**, and **MAC Address**.

The Wi-Fi Access Point panel contains four fields: **Link Status**, **IP Address**, **Netmask**, and **MAC Address**. The Wi-Fi Connected Clients panel contains six fields: **MAC Address**, **IP Address**, **Average RSSI**, **Connect Time**, **Authorized**, and **Authenticated**. See Figure 12 on page 12.

Click on the **Refresh** button to update the information displayed on the *General Status* screens.
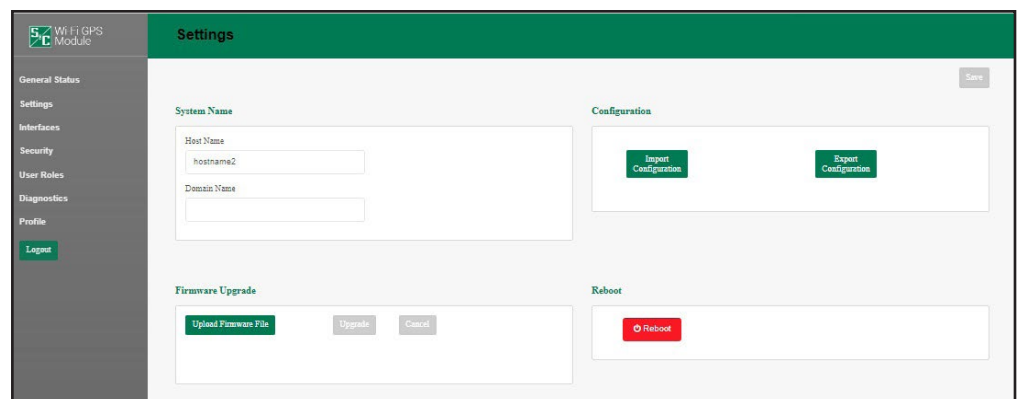

Figure 13. The System Name and Firmware Upgrade panels on the *Settings* screen.

Settings

Click on the **Settings** menu item in the left menu to open the *Settings* screen. See Figure 13.

The *Settings* screen contains the System Name, Firmware Upgrade, Configuration, and Reboot panels.

NOTICE
When a field edit is typed, the **Save** button becomes green and must be clicked on to save the new entry.

System Name

Enter a user-defined name for the **Host Name** setting and click on the **Save** button. The **Name** fields are limited to 50 characters. The entry in the **Host Name** field is displayed in the **Name** field on the *General Status* screen. The **Domain Name** field is not used.

Firmware Upgrade

This panel enables loading a firmware version onto the R3 Communication Module.

Follow these steps to perform a firmware upgrade:

STEP 1. Download the firmware file to the computer and note the firmware version. The firmware files are located in the S&C Customer Portal at **sandc.com/en/support/sc-customer-portal/**.

STEP 2. Click on the **Upload Firmware File** button in the Firmware Upgrade panel.

STEP 3. A Windows dialog box appears. Navigate to and select the required firmware file. The file will upload to the R3 Communication Module. When the upload has completed, the successful upload is confirmed. Then, the Wi-Fi/GPS module verifies S&C Electric Company securely digitally signed the installer.

STEP 4. After verification, a notification appears. Click on the **OK** button to dismiss the notification.

STEP 5. When the **Upgrade** button becomes active, click on it. This starts the upgrade process.

STEP 6. When the upgrade process completes, a notification appears. Click on the **OK** button. The R3 Communication Module will be unavailable while it reboots. The reboot takes approximately 5 minutes, and the *Login* screen opens when the reboot is complete.

STEP 7. Log in and confirm the new firmware has been installed successfully by checking the *General Status* screen.

Configuration Files

The R3 Communication Module can perform bulk imports and exports of specific configuration data parameters. The same XML file format is used for both import and export functions. This allows a user to configure settings in one device, export the settings into an XML file (with the extension .json), and import the same settings into another communication module.

Clicking on the **Import Configuration** or **Export Configuration** button invokes a series of dialog boxes allowing navigation on a PC to a configuration file for import or saving a file for export. See Figure 14.
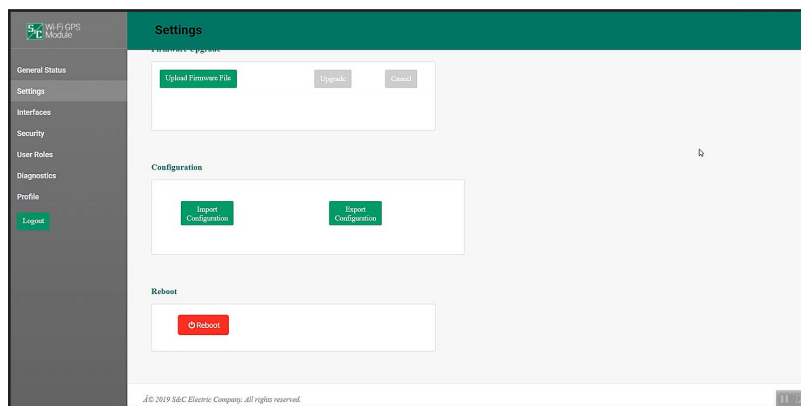

Figure 14. The Configuration and Reboot panels on the *Settings* screen.

Import Configuration

Follow these steps to complete the **Import Configuration** command:

STEP 1. In the Configuration panel, click on the **Import Configuration** button. A Web User Interface (WUI) dialog box appears.

STEP 2. Click on the **Choose File** button. A Windows file navigation box will open.

STEP 3. Navigate to the file.

STEP 4. Highlight the file and click on the **Open** button. The highlighted file will be identified in the WUI dialog box.

STEP 5. Click on the **Import** button.

STEP 6. Click on the **Save** button.

Export Configuration

Follow these steps to complete the **Export Configuration** command:

STEP 1. In the Configuration panel, click on the **Export Configuration** button. A WUI dialog box appears with a suggested filename for the exported configuration. The default name is "textFile," but it can be changed.

STEP 2. Click on the **Export** button.

STEP 3. Wait a few seconds for the exported file to open in the browser. The file will be stored in the Downloads folder.

Reboot

The red **Reboot** button enables the user to restart the communication module. When selected, a dialog box appears for confirmation of the **Reboot** command. After clicking on the **OK** button, the user interface shows an Unavailable dialog box. The reboot process requires approximately 5 minutes before communication to the R3 Communication Module is re-established. When the reboot is complete, the *Login* screen will open.
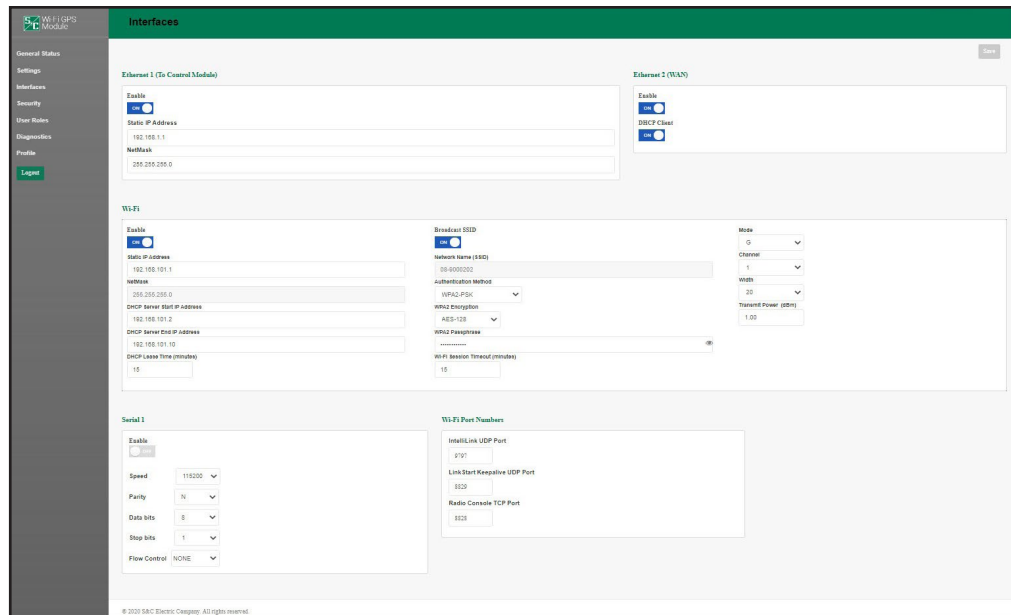
Interfaces

Figure 15. The default *Interfaces* screen.

Ethernet 1 (To Control Module)

In this panel, the network associated with the communication module local area network (LAN) is defined for devices connecting to physical Ethernet Port 1. See Figure 15. The R3 Communication Module ships with a default IP address of 192.168.1.1 and a Netmask equal to 255.255.255.0.

NOTICE
The R3 Communication Module must be configured for Ethernet IP wiring. See S&C Instruction Sheet 766-526 for more information.

Ethernet 2 (WAN)

This panel defines the IP addressing for the R3 Communication Module's Ethernet Port 2 and subsequent network linkage and settings respective to the customer's legacy backhaul WAN network. The default setting is **DHCP Enabled**.

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

DHCP Client State "On"

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

DHCP Client State "Off"

Three fields require identification: **Static IP Address**, **Default Gateway IP Address**, and **Netmask**. The **Static IP Address** setpoint is the WAN IP address assigned to the R3 Communication Module. The **Default Gateway IP Address** setpoint is the address of the network device upstream of the R3 Communication Module and determines the destination of DNP3 traffic sent to the SCADA master(s). See Figure 16.

The address entries are automatically verified to ensure they function with the other values entered.
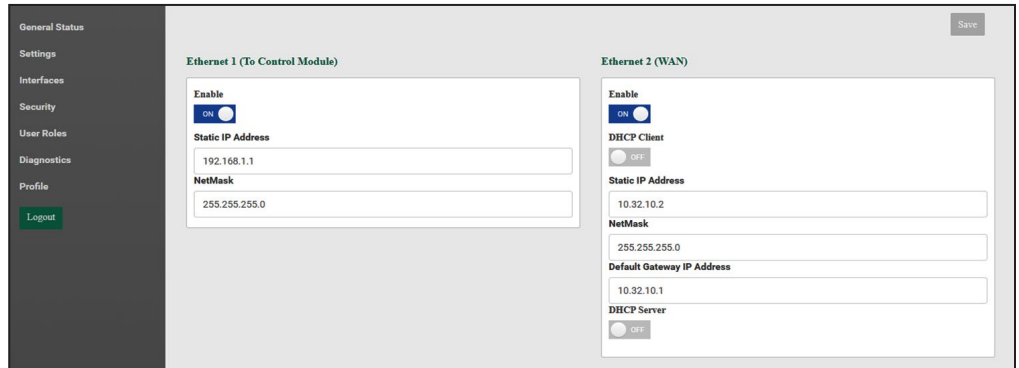
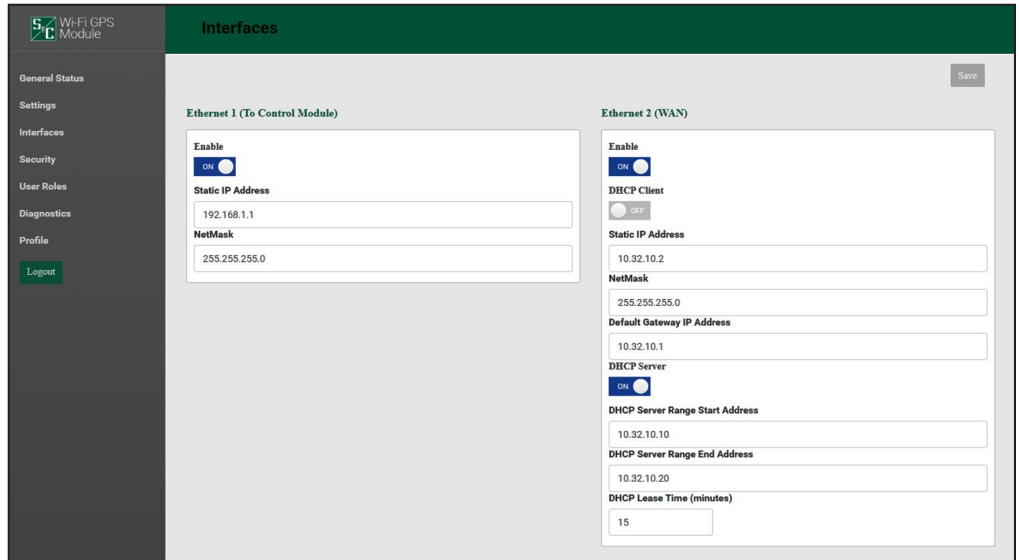**Figure 16. The *Interfaces* screen with the DHCP client disabled.**

Figure 17. The *Interfaces* screen with the DHCP client disabled and the DHCP server enabled.

DHCP Server State "On"

When the DHCP client is disabled, the DHCP server can be enabled. This allows the R3 Communication Module to automatically provide an IP address to an attached device, such as a field area network radio. See Figure 17 on page 17.

Wi-Fi

The Wi-Fi panel is comprised of the **Enable** and **Broadcast SSID** buttons, and the **Static IP Address**, **Netmask**, **DHCP Server Start IP Address**, **DHCP Server End IP Address**, **DHCP Lease Time (minutes)**, **Network Name (SSID)**, **Authentication Method**, **WPA2 Encryption**, **WPA2 Passphrase**, **Mode**, **Channel**, **Width**, and **Transmit Power (dBm)** fields. See Figure 18.

The communication module ships with a default Static IP address of 192.168.101.1, a Netmask equal to 255.255.255.0, a DHCP server Start IP address of 192.168.101.2, a DHCP Server End IP address of 192.168.101.10. See Figure 18. The Broadcast SSID is in the **Off** position. The **Network Name (SSID)** setting is factory configured with the IntelliRupter fault interrupter serial number. The default **Authentication Method** setpoint is WPA2-PSK default.

When the **Authentication Method** setpoint is in the **WPA2-PSK** setting, an additional **WPA2 Passphrase** field displays. Enter the passphrase required to open a Wi-Fi connection with this IntelliRupter fault interrupter serial number. The **Wi-Fi Session Timeout** field determines the time after which the session will automatically terminate from inactivity through the connections.

The **Mode** setting selects the preferred Wi-Fi transmission standard (Default: N). The **Channel** setpoint can be set to a channel with less traffic. The **Width** setpoint is the channel bandwidth in MHz. This setting is only relevant when 802.11n is chosen for the **Mode** setting. It will be ignored if 802.11b or 802.11g is selected.
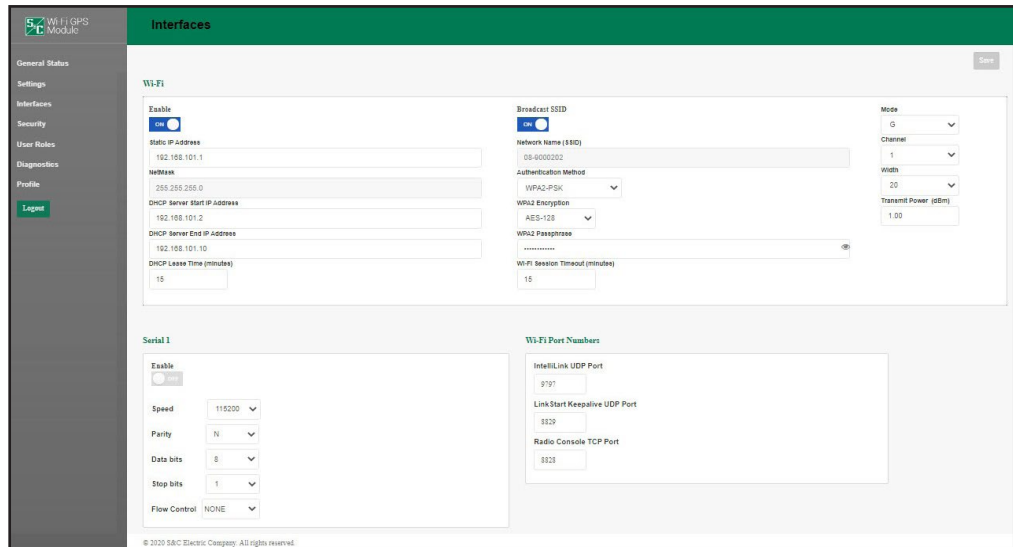

Figure 18. The default *Interfaces* screen Serial 1 and Wi-Fi Port Numbers panel.

Serial 1 (DB9 Port)

This is the RS-232/DB9 port for connection to the radio's serial console port. If use of RTS/CTS is required, set the **Flow Control** setpoint to "NONE." See Figure 18 on page 18.

Wi-Fi Port Numbers

This section displays three configurable port numbers the R3 Communication Module uses to receive packets via the Wi-Fi interface.

Enter the IntelliLink® software UDP Port number and the Radio Console TCP Port number.

The IntelliLink software UDP port is used to receive local packets from a device attached via Wi-Fi. This port has a valid range of 1024-65535, and a default of 9797.

The LinkStart Keepalive UDP port is used to provide connection information to the LinkStart desktop application on the user's device. This port has a valid range of 1024-65535 and a default of 8829.

The Radio Console TCP port is used to receive packets from a Wi-Fi device intended to be redirected to the serial console interface of a field area network radio device. These packets are directed through the R3 Communication Module's DB9 port to the radio device. This port has a valid range of 1024-65535, and a default of 8828.

Note: When modifying any of these port values, the similar configuration settings in the LinkStart desktop application must also be modified. In LinkStart, click on the **Tools** tab, and then select "TCP/IP Port Options." Three similar settings must be set to the same values as the port numbers in the R3 Communication Module. In LinkStart, the R3 IntelliLink UDP port corresponds to the communication module's IntelliLink UDP port, the R3 Keepalive UDP port corresponds to the LinkStart Keepalive UDP port, and the R3 VCOM TCP port corresponds to the Radio Console TCP port.
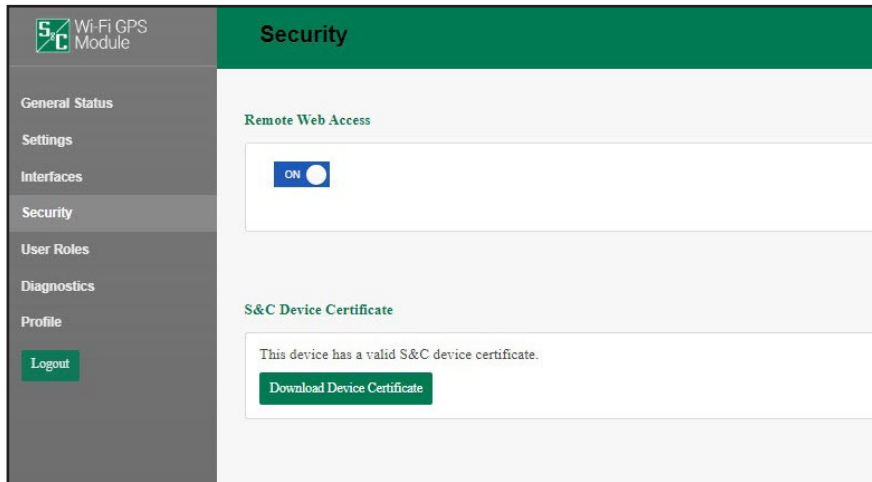
Security

Figure 19. The *Security* screen.

Remote Web Access

The **Remote Web Access** toggle button enables Web-user interface access via Ethernet Port 2.

To access the user interface for Wi-Fi Administration through the field area network, set the **Remote Web Access** setpoint to "on." See Figure 19.

Note: The **Remote Web Access** setpoint is not available until the default admin password is changed, and remote access requires the field area network to be routed through the Wi-Fi/GPS module by using the Ethernet wiring configuration.

NOTICE
When a SpeedNet Radio is 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 maximum transmission unit (MTU) 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, use the following command on a Windows 10 machine: **netsh interface ipv4 set subinterface "Local Area Connection" mtu=500 store=persistent**.

S&C Device Certificate

Under "S&C Device Certificate," the Web page will display a message indicating whether this R3 Communication Module device has a valid factory-assigned S&C Device Certificate. A valid certificate is required to allow this R3 Communication Module to securely pair with an R3 Control Module and enable faster IntelliLink software local traffic. If the R3 Communication Module has a valid certificate, click on the **Download Device Certificate** button to retrieve and view the details of the certificate. If the R3 Communication Module does not have a valid certificate, call S&C's Global Support and Monitoring Center at 1-888-762-1100 for additional instructions.

User Roles

The *User Roles* screen permits adding and editing users and their access privileges. The types of user roles include Admin, Engineer 1, Technician 1, and Viewer. The addition of a user is initiated by clicking on the **Add User** button. A dialog box appears with the required **User**, **Password**, and **Confirm Password** fields, and a drop-down box to select the user **Role** setpoint.

Clicking on a user entry in the list opens the dialog box to edit information for that user. See Figure 20. The permissions provided to each of the user roles are summarized in Table 1 on page 22.

The Admin Role column is assigned to the system administrator, who is not included in this list and therefore cannot be removed. The **User Roles** menu item in the left menu is only available for use by the system administrator (Admin Role) and Additional Admin Role users.
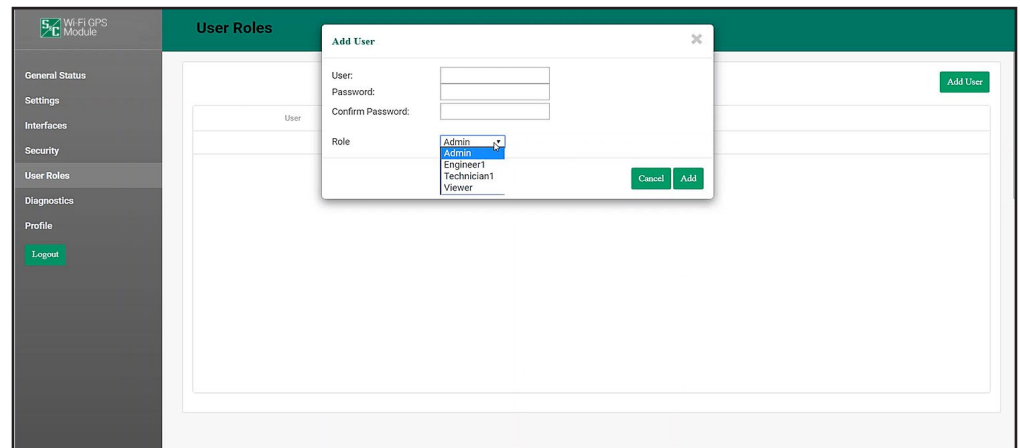

Figure 20. The *User Roles* screen.

Table 1. User Role Permissions

Page	Element Within Page	Admin Role	Addi-tional Admin Role	Engineer 1 Role	Technician 1 Role	Viewer Role
General Status	All	Allowed	Allowed	Allowed	Allowed	Allowed
Settings	Update Gateway Names, Import/ Export Configurations	Allowed	Allowed	Allowed	Allowed	Blocked
	Install Firmware	Allowed	Allowed	Allowed	Allowed	Blocked
Interfaces	All	Allowed	Allowed	Allowed	Blocked	Blocked
Security	Install Web Server Certif-icate	Allowed	Allowed	Blocked	Blocked	Blocked
	Enable Remote Web Access	Allowed	Blocked	Blocked	Blocked	Blocked
User Roles	All	Allowed	Allowed	Blocked	Blocked	Blocked
Diagnostics	All	Allowed	Allowed	Allowed	Allowed	Allowed
Profile	All	Allowed	Allowed	Allowed	Allowed	Allowed

Diagnostics

The *Diagnostics* screen initiates the retrieval of the Diagnostic and Event Log files. See Figures 21 and 22.
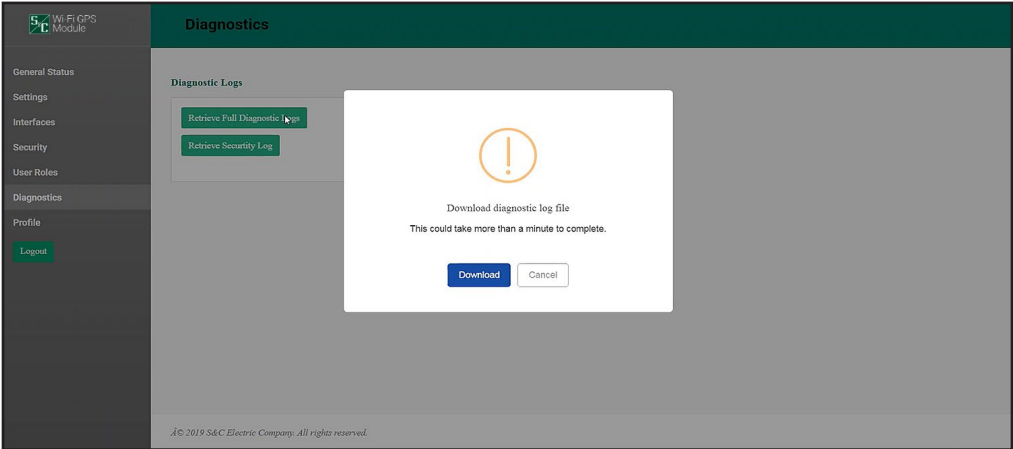
Figure 21. The Retrieve Full Diagnostics Logs button on the *Diagnostics* screen.
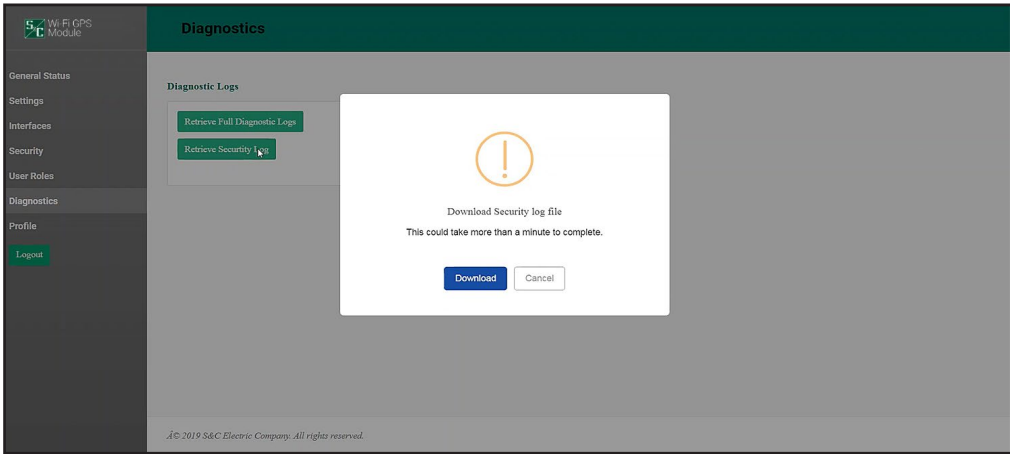
Figure 22. The Retrieve Security Log button on the *Diagnostics* screen.

Profile

The *Profile* screen enables the present user logged in to the R3 Communication Module to change password credentials. See Figure 23.
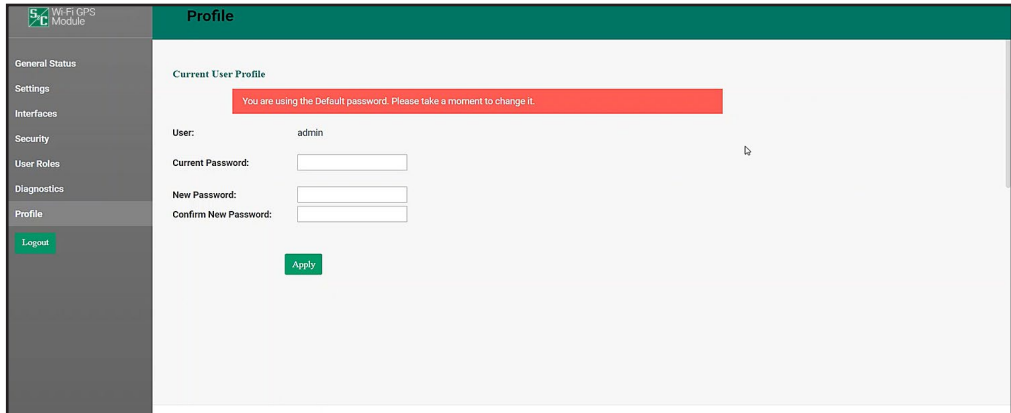

Figure 23. The *Profile* screen.

The password entry must be at least eight characters in length, with one lowercase and one uppercase character. When entries are complete, click on the **Apply** button to save the new password.

Logout Button

Clicking on the **Logout** button in the left menu closes the Wi-Fi Administration program and returns to the *Wi-Fi Connection Management* screen.

Configuration

The R3 Communication Module is a direct replacement for the R0 communication module. This is the default wiring for the R3 Communication Module. See Figure 24 and Figure 25 on page 26.

To obtain remote access to the Wi-Fi/GPS User Interface the WAN must be routed through the Wi-Fi/GPS module. Doing so will enable remote firmware updates and will be required for some cybersecurity features provided in future releases of the Wi-Fi/GPS firmware.

To configure the R3 Communication Module with the alternate wiring needed to route WAN traffic through the Wi-Fi/GPS, follow the steps in S&C Instruction Sheet 766-526, "IntelliRupter® PulseCloser® Fault Interrupter, *R3 Communication Module Retrofit and Configuration.*"

Interface Pinouts

The RS-232 Radio Maintenance Port of the R3 Communication Module is configured as data-terminal equipment. See Figure 24.

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
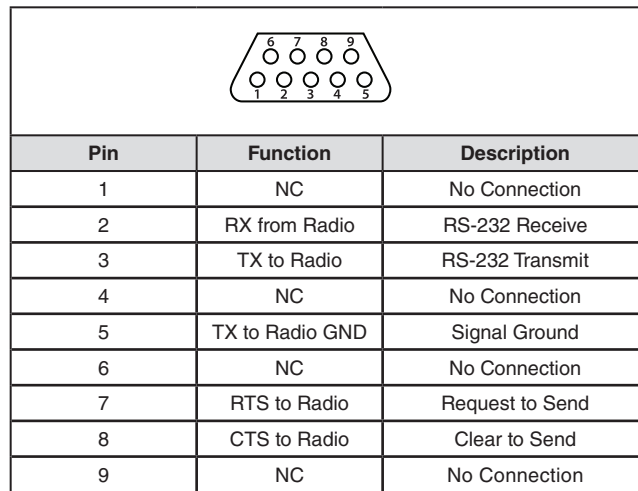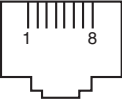
Figure 24. The R3 Communication Module RS-232 interface pinout.

The R3 Communication Module Ethernet ports use RJ-45 connectors with the pinout shown in Figure 25. 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.

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

Figure 25. The R3 Communication Module RJ-46 interface pinout.

NOTICE
When a SpeedNet Radio is 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 maximum transmission unit (MTU) 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 on a Windows computer, open a command prompt in **Administrator** mode and follow these steps:

STEP 1. Open a Command prompt by typing run in the Windows Search prompt and then type "cmd" in the Open: dialog box. Then, hold the <Ctrl>, <Shift>, and <Enter> keys to run the Command prompt with Administrator access. See Figure 26.

Note: If this is not allowed, the user does not have administrative rights to the computer and will be unable to change the MTU as needed.
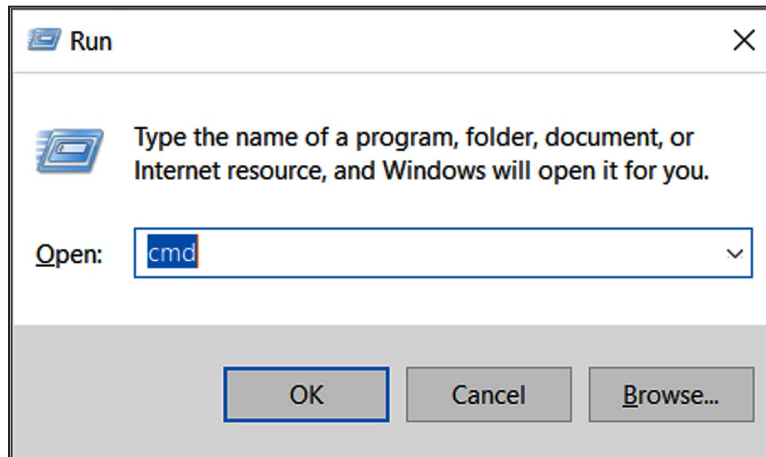
Figure 26. Running the Windows command prompt.

STEP 2. In the Command prompt, type "ipconfig" and look for the communication adapter/interface to be used to connect to the R3 Communication Module remotely. Typically, this will be one of the Ethernet adapters or a wireless local area connection adapter. See Figure 27.

```
Command Prompt
Microsoft Windows [Version 10.0.19042.1766]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\System32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . :
   Subnet Mask . . . . . . . . . . . :
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 3:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . :
   Subnet Mask . . . . . . . . . . . :
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

Figure 27. The Windows "ipconfig" command output example.

STEP 3.   Now type the following command: "netsh interface ipv4 set subinterface "interface name" mtu=500 store=persistent". Replace the "interface name" with the actual name of the interface being used for the remote connection. As an example, if the Windows computer was using the Ethernet 3 interface, the command would be: "netsh interface ipv4 set subinterface "Ethernet 3" mtu=500 store=persistent". See Figure 28.
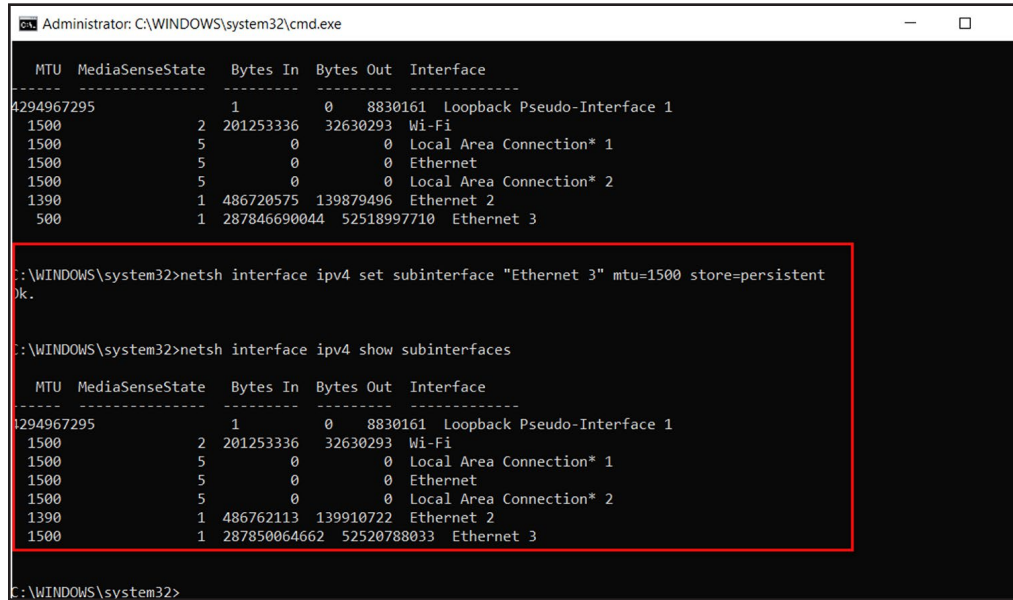
Figure 28. Executing the "netsh" command to change the MTU example.

STEP 4.   To verify the MTU changed, type "netsh interface ipv4 show subinterfaces", and look for the subinterface that was changed, and verify the MTU is now 500. See Figure 29.

Figure 29. Verifying the MTU changed example.

STEP 5. If desired, to change the MTU back to 1500 afterward, type: "netsh interface ipv4 set subinterface "interface name" mtu=1500 store=persistent". Replace the "interface name" with the actual name used in the previous steps. To verify the MTU changed back to 1500, type: "netsh interface ipv4 show subinterfaces". Look for the subinterface that was changed and verify the MTU is now 1500. See Figure 30.

Figure 30. Verifying the new MTU changed example.